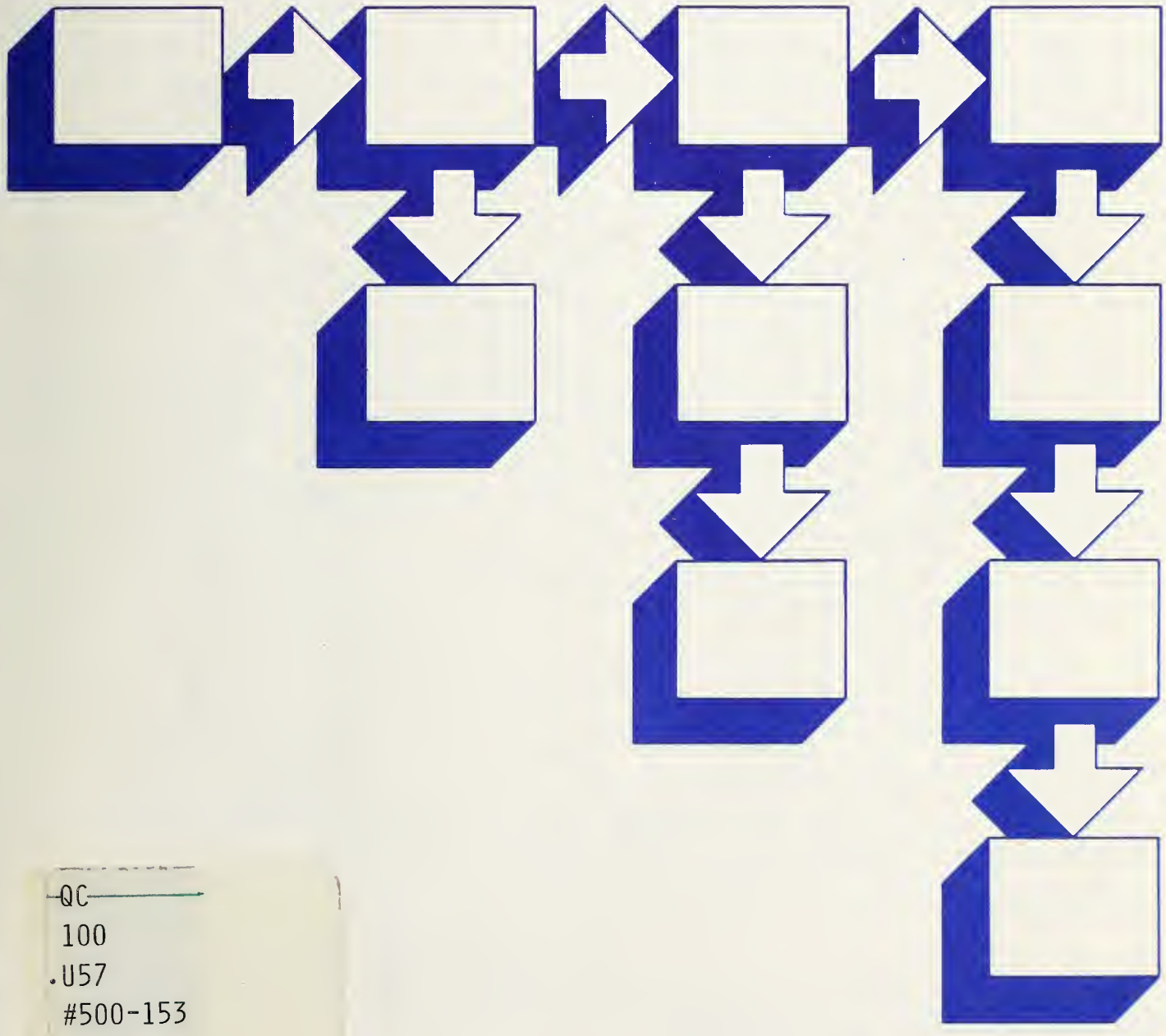
Computer Science and Technology

NBS Special Publication 500-153

Guide to Auditing for Controls and Security: A System Development Life Cycle Approach



The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NBS work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the Institute for Computer Sciences and Technology, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

The Institute for Computer Sciences and Technology

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Computer Systems

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Bureau-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following Divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3]Located at Boulder, CO, with some elements at Gaithersburg, MD

Computer Science and Technology

NBS Special Publication 500-153

Guide to Auditing for Controls and Security: A System Development Life Cycle Approach

Editors/Authors: Zella G. Ruthberg
Bonnie T. Fisher
William E. Perry
John W. Lainhart IV
James G. Cox
Mark Gillen
Douglas B. Hunt

Co-Sponsored by:
President's Council on Integrity and Efficiency
and
Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

April 1988

U.S. DEPARTMENT OF COMMERCE
C. William Verity, Secretary

National Bureau of Standards
Ernest Ambler, Director

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 88-600518
National Bureau of Standards Special Publication 500-153
Natl. Bur. Stand. (U.S.), Spec. Publ. 500-153, 266 pages (Apr. 1988)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1988

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington DC 20402

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ADP	Automated Data Processing
AIS	Automated Information System
CFR	Code of Federal Regulations
COTR	Contracting Officer's Technical Representative
DP	Data Processing
EDP	Electronic Data Processing
FAR	Federal Acquisition Regulation
FIRMR	Federal Information Resources Management Regulation
FPR	Federal Procurement Regulation
FPMR	Federal Property Management Regulation
GAO	General Accounting Office
GSA	General Services Administration
ICS	Internal Control Specialist
OIG	Office of Inspector General
OMB	Office of Management and Budget
NBS	National Bureau of Standards
PCIE	President's Council on Integrity and Efficiency
PCMI	President's Council on Management Improvement
PM	Project Manager
QA	Quality Assurance
RFP	Request for Proposal
SDLC	System Development Life Cycle
SDM	System Development Methodology
SLC	System Life Cycle
SSS	System Security Specialist
VV&T	Verification, Validation, and Testing

EXECUTIVE SUMMARY

This guide addresses auditing the system development life cycle (SDLC)* process for an automated information system (AIS), to ensure that controls and security are designed and built into the system. The guide also presents a process for deciding which system to audit among an organization's universe of systems. It is directed toward mid-level ADP auditors having a minimum of two years experience in ADP auditing, but can also be used by security reviewers, quality assurance personnel, and as a training tool for less experienced ADP auditors. ADP managers and system developers will also find it useful guidance on security and control issues. The guide is designed to provide audit/review programs for each major phase of the SDLC process and assumes a large sensitive system. The reader is expected to make appropriate modifications for small less sensitive systems. The guide represents the results of the past four years of activities by the Electronic Data Processing (EDP) Systems Review and Security Work Group of the Computer Security Project within the President's Council on Integrity and Efficiency (PCIE). (See Appendix A for more information on the Work Group.)

This guide can be used in any of the following ways:

1. Understanding the need for and planning for audit or review involvement in AISs under development - Chapters 1 and 2 are designed to assist the auditor in planning an audit for such systems under development. These chapters explain the new or increased risks in AISs, the types of controls used in those systems, as well as a conceptual model for systems development.

2. Identifying systems for audit/review involvement - Chapter 3 provides a risk assessment approach to help identify an agency's high-risk systems. These are the systems most needing audit/review coverage.

3. Creating a phase-by-phase program for auditors or security reviewers involved in a review of AISs under development - Chapter 4 provides a complete audit/review program designed for each of the five major phases of the system development process.

* Throughout this document, the system development life cycle (SDLC) is defined as a major subset of the system life cycle (SLC). The SLC consists of the five phases in the SDLC plus the sixth phase, Installation and Operation.

In order to provide a rich background of materials for the user of the guide, the relevant laws and regulations are cited and described (Section 1.1.5 and Appendix B) and the most useful references are cited with many of them described (Sections 2.2.1.2.1 and 2.2.1.2.2, Appendices G and H). The relevant laws regulations, and standards promulgated by Congress, the Office of Management and Budget (OMB), and the U.S. General Accounting Office (GAO) have been divided into two sets: 1) those that require audit involvement in AISs and 2) those that require internal control in AISs. Chapter 1 also contains a discussion of the related issues of computer generated risk, control objectives and standards in a computer environment, the audit/review evidence found in automated systems, and AIS auditability. The references appearing in Chapter 2 of the guide are also divided into two sets: 1) those NBS and DOD documents that formed the basis for the Life Cycle Matrix of Figure 1 and 2) the major related General Services Administration (GSA) references on software improvement and software engineering. Appendix G contains descriptions of key references relating to all the materials in this guide while Appendix H contains a more general listing of related references, with no descriptions.

The model arrived at for describing the phases and functional roles in the AIS life cycle is presented in the Life Cycle Matrix in Figure 1 and described at length in Chapter 2. The accompanying flow of documents, as the system progresses through the life cycle phases of Initiation, Definition, Design, Programming and Training, Evaluation and Acceptance, and Installation and Operation, are shown in Figure 2 and described in Section 2.6. The activities to be conducted by the functional roles (i.e., Information Resources Management Official, System Security Officer/Internal Control Officer, Auditor, Sponsor/User, Project Manager/Contracting Officer's Technical Representative, System Security Specialist, Internal Control Specialist, Contracting Officer, ADP Manager, and Quality Assurance Specialist) appear in abbreviated form in the Life Cycle Matrix of Figure 1 and are described more fully in Section 2.4. Changes in these activities that result from the use of external development services (contract or off-the-shelf) are discussed in Section 2.5.

Since ADP audit or security reviews can be very time consuming and, therefore, can place a tremendous drain on an organization's audit/review resources, the Work Group developed a work priority scheme in March of 1986, using the input generated by a small invitational workshop on the subject. This scheme was published as an internal report by the National Bureau of Standards in August of 1986, NBSIR86-3386, and appears in this guide as Chapter 3. The scheme is in the form of a high level risk assessment which employs a two-level review of the major areas of concern (or dimensions). Level I looks at the dimension called Criticality/Mission Impact while Level II looks at four dimensions (namely, Size/Scale/Complexity, Environment/Stability, Reliability/Integrity, and Technology Integration). The result of applying the scheme is to rank the audit/review work in order of degree of risk posed to the organization by the various AISs. Information from existing risk analyses and vulnerability assessments may be used to reduce the costs of this risk assessment.

Chapter 4 presents an audit/review program for each of the five phases of the system development process (SDLC). The control objectives used as the basis for each phase audit/review are divided into six categories (i.e., Legal Requirements, Management Policies, Internal Controls, Audit Trails, Documentation, and Economy and Efficiency) and are taken from the U.S.GAO "Yellow Book" on standards for audit in the Federal government [GAO81-1]. The contents of each phase audit/review program are driven by the listing of activities found in the Life Cycle Matrix of Figure 1. The first step in the audit/review program is to evaluate the life cycle methodology currently being used by the organization, to ensure that it encompasses the best parts/documents of the methodology described in Chapter 2. The audit/review coverage in each phase is presented in a parallel manner for consistency and equal comprehensiveness. Each phase audit/review effort is presented in terms of the same eight components: 1) brief introduction to the phase and appropriate audit participation, 2) primary audit objectives, 3) overview of the phase, 4) initial background audit survey, 5) customized audit objectives, 6) detailed audit testing, 7) assessment of audit results, and 8) questionnaires or matrices for obtaining information (the audit program), found in Tables 4.1 to 4.5.

Although quality assurance is not heavily implemented in the Federal agencies at this time, the quality assurance functional role was included because use of this activity, in early system development particularly, can greatly reduce costly errors and omissions as well as the agency's audit burden. Given the relatively limited amount of resources available for ADP reviews and the time consuming nature of ADP systems development work, auditors should focus heavily on 1) the effectiveness of the process for designing and developing internal controls in automated systems and 2) the substance of those internal controls. These reviews would result in large cost savings for the organizations.

Any rigid application of the SDLC process presented here would be unrealistic in the rapidly changing computer environments that may now include such elements as distributed databases, expert systems, protyping, and computer-aided systems engineering. The reader is urged to be flexible and to follow the spirit of this document in such instances, rather than adhere blindly to the details in this guide.

Although operational audits are also important, they are not addressed because there is already much public literature on that subject. For control assessment in the operational phase, the GAO "Black Book" [GAO81-3] has a particularly thorough treatment. The main reasons for choosing to address SDLC audit are 1) there is a tremendous pay-off available to an organization when systems are developed with controls and security from the start and 2) there is currently very little comprehensive guidance available on SDLC audits for the Federal government. The Work Group hopes this document helps to fill this need.

ACKNOWLEDGEMENTS

This document represents the efforts of many people. The list of editors/authors cites the individuals who contributed most to the final contents. Bonnie T. Fisher was primarily responsible for the Life-Cycle Matrix described in Chapter 2 and co-authored, with Zella G. Ruthberg, the Work Priority Scheme found in Chapter 3. William E. Perry wrote the initial draft of the body of the document, under contract to the Institute for Computer Sciences and Technology (ICST) at the National Bureau of Standards (NBS) and the Office of Inspector General (OIG) of the Department of Health and Human Services (HHS). Still under contract, he also wrote the second draft, using extensive revisions recommended by John W. Lainhart IV, James G. Cox, Mark Gillen, and Douglas B. Hunt as well as Bonnie T. Fisher and Zella G. Ruthberg. The third and final draft was the result of many hours spent by this subcommittee of the EDP Systems Review and Security Work Group (the editors/authors minus W. E. Perry).

During the latter half of this project, Gail Shelton and James G. Cox were the project leaders of the EDP Systems Review and Security Work Group under Richard Kusserow, Inspector General of HHS. Ms. Shelton very ably planned and carried out the many administrative details of this complex undertaking while Mr. Cox handled the technical component. We would like to thank them both for their efforts in these capacities. Finally, James E. Lebo, a Co-operative Education student with ICST/NBS converted the document into a desk top publishing format and produced the very professional looking printing of the text. We would like to thank him for his resourcefulness in accomplishing this in a conscientious and timely manner.

Zella G. Ruthberg
Computer Scientist, ICST/NBS
October 30, 1987

CHAPTER 1
GENERAL ADP AUDIT ISSUES

1.1 INTRODUCTION

1.1.1 Scope of the Audit Guide

Auditing in a computerized environment covers a broad spectrum of activities. The activities range from using reports produced by computerized applications, to assessing the adequacies of controls in sophisticated information systems, to evaluating automated information systems (AISs) under development. The range of skills needed to audit successfully in a computerized environment varies as greatly as the activities audited.

This guide covers auditing the system development life cycle (SDLC)[1] process for a system, to ensure that controls and security are designed into the system. The guide also presents a process for deciding which system to audit among an organization's universe of systems. It is directed toward mid-level ADP[2] auditors having a minimum of two years experience in ADP auditing, but can also be used by security reviewers, quality assurance personnel, and as a training tool for auditors with less experience in ADP auditing. ADP managers and system developers will also find it useful guidance on security and control issues. The guide is designed to provide audit/review programs for each major phase of the SDLC and assumes a large sensitive system. The reader is expected to make appropriate modifications for a small less sensitive system.

Section 2.3 of this guide defines an SDLC that encompasses generally accepted phases used in many Federal agencies. Each phase of this life cycle is defined there. The roles of the participants, including the auditor[3], are also defined. The audit role for each life cycle phase is supported by an audit program in Chapter 4, including questionnaires for use by the auditor during that phase. The GAO "Black Book" [GAO81-3] provides a control assessment approach for evaluating general and application controls in an operational computer-based environment.

---

1 Throughout this document, the system development life cycle (SDLC) is defined as a major subset of the system life cycle (SLC). The SLC consists of the five phases in the SDLC plus the sixth phase, Installation and Operation.

2 Electronic Data Processing (EDP) is the term commonly used in the private sector. However, since the Federal government uses the broader term Automatic Data Processing (ADP) instead of EDP, and since this document is being produced by the Federal government, this document will conform to Federal usage and use ADP whenever there is a choice.

3 The terms 'auditor' and 'audit' are used throughout this document without the qualifiers 'internal' or 'external' since this guide can be used by both types.

1.1.2 How to Use the Audit Guide

This audit guide is designed to be used as an audit program for auditing AISs under development. It can be used in any of the following ways:

1. Understanding the need for and planning for audit involvement in AISs under development - Chapters 1 and 2 are designed to assist the auditor in planning an audit for such systems under development. These chapters explain the new or increased risks in AISs, the types of controls used in those systems, as well as a conceptual model for systems development.
2. Identifying systems for audit involvement - Chapter 3 provides a risk assess-ment approach to help identify an agency's high-risk systems. These are the systems most needing audit coverage.

3. Creating a phase-by-phase program for auditors involved in a review of AISs under development - Chapter 4 provides a complete audit program designed for each of the five major phases of the system development process.

1.1.3 Auditor Skills Needed

Audits of systems under development require skills beyond those needed to conduct non-ADP audits of lesser scope. Because the system is under development, the auditor must often assess how well a project is being managed, the adequacy of planning, or the standards being followed. To do this, the auditor must have knowledge and experience in such areas as:

1. System development methodologies;

2. Standards for system documentation and software engineering;

3. Systems planning and project management methods; and

4. Methods, procedures, or standards for developing, documenting, and testing controls.

These skills have been laid out as job core dimensions by the EDP Auditors Foundation, Inc.[4], The skills are also those needed for certification as an information system auditor (CISA). Generally, auditors who 1)have mastered the CISA job core dimensions, 2)have met

---

4 See Exhibit I in "Information Systems Audit Process," by S. R. Vallabhaneni [VALLS83] for a concise picture of the job dimensions for a Certified Information Systems Auditor (CISA) and their relation to the information systems audit function. See Appendix G for more information on the document.

the prerequisites for the CISA, and 3)have continued their education program then have the skills needed for auditing systems under development.

Where particular skills are lacking, it is still possible to do useful ADP audit work. The scope of the audit, however, should probably be restricted (e.g., if skills in controls are strong but skills in systems management are weak, the audit might be properly restricted to control issues). An alternative is to team up such an auditor with a person in the organization having the missing skills and not involved in the system under review.

1.1.4 Auditing in a Computerized Environment

1.1.4.1 The Need - The computer has substantially altered the methods by which processes, such as payroll and accounts receivable, operate and are controlled and audited. The opportunities for personal review and clerical checking have declined as the collection and subsequent uses of data are changed. The changes are the result of moving from manual procedures performed by individuals familiar with both the data and the accounting process, to high volume, automated techniques performed by individuals unfamiliar with either the data or the accounting practices.

Computerization has substantially reduced the time available for the review of transactions before their entry into the automated system's records. As a result, in poorly controlled systems the opportunity for discovering errors or fraud before they have an impact on operations may be reduced, especially in the case of real-time and data base systems. This has increased the importance of internal control/security procedures. Thus, it is imperative that the auditor review these systems as they are being developed, to insure that adequate controls and security are designed into the system from the outset.

1.1.4.2 The Scope of Audit in a Computerized Environment - Auditing in a computerized environment can be divided into two broad areas. First is the audit of operational computer systems, and second is the audit of systems under development. These two types of audits require significantly different approaches.

The audit of operational systems evaluates the results of operations. It is normally a data-oriented audit, looking at processed transactions. Controls can be evaluated by examining the results of operation.

In a developmental audit, there is no operational system or data. The auditor evaluates controls without the benefit of observing processing results. In addition, in a developmental audit the auditor is concerned with ensuring that the developmental procedures and standards have been properly followed. As stated earlier, this guide addresses developmental audits only.

1.1.4.3 Relationship Between Systems Development Audits and Operational Audits of Automated Information Systems (AISs) - The operational audit can identify AIS vulnerabilities, but these may not be correctable after development because of the associated costs. Studies have shown that it costs approximately 50-100 times more to correct an operational system as it would have cost to build in the necessary control during development.

If the auditor can identify potential vulnerabilities during development, they can be more easily and economically corrected than after the AIS is installed and operational. Thus, it becomes imperative to evaluate the adequacy of the developer's approach to controls, i.e., how controls are addressed, implemented, and documented. When an adequate system of controls is built in during development, it can be fine-tuned through operational audits, as necessary.

The developmental audit team should define operational audit programs, areas for review during operations, and recommend specific audit tools and techniques for use during operational audits. The developmental audit team can, therefore, play a significant role in making operational audits of systems more effective, efficient, and economical.

1.1.5 Relevant Laws and Regulations

Congress and Federal regulatory agencies have grown increasingly concerned about the integrity of Federal computerized systems. This concern also covers the security and privacy of data stored by Federal computer systems. The relevant laws, regulations, and standards include the following: (Note that longer descriptions can be found in Appendix B.)

1.1.5.1 Requirements for Audit Involvement - The laws, regulations, and guidance pertaining to the performance of the audit function, particularly as related to AIS audits, are briefly described below:

1. Inspector General Act of 1978 (PL95-452) [IGA78] - Establishes the Offices of Inspector General in many major Federal agencies and specifies their audit and investigative responsibilities.

2. Standards For Audit of Governmental Organizations, Programs, Activities, and Functions, by U.S. General Accounting Office (GAO), 1981 [GAO81-1] - Defines the standards for the conduct of Federal audits.

3. Quality Standards for Federal Offices of Inspector General, by President's Council on Integrity and Efficiency (PCIE), 1986 [PCIE86] - Provides quality standards for management, operation, and conduct of the Federal Offices of Inspector General.

4. Budget and Accounting Procedures Act of 1950 (PL81-784) [BAPA50] - Specifies detailed audit objectives for GAO conducted audits.

1.1.5.2 Requirements for Internal Control - The laws, regulations, and guidance describing control required for agencies and systems, including the responsibility for control, are listed and briefly described below:

1. Budget and Accounting Procedures Act of 1950 (PL81-784) [BAPA50] - Requires that agency heads establish and maintain effective systems of internal control.

2. Brooks Act (PL89-306), 1965 [BRA65] - Provides for the "economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies."

3. Freedom of Information Act (PL93-502), 1974 [FIAA74] - Establishes procedures under which an individual can obtain records in the possession of the Federal government while enabling the government to protect records that require confidential treatment.

4. Privacy Act of 1974 (PL93-579) [PYA74] - Establishes standards and safeguards for the collection, maintenance, or disclosure of an individual's personal information by Federal agencies, and grants an individual access to the records concerning him/her maintained by Federal agencies.

5. Federal Records Management Acts (PL81-754, PL94-575), 1950 [FRMA50] and 1976 [FRMA76] - Require establishment of standards and procedures to ensure effective records creation, use, maintenance, and disposal.

6. Paperwork Reduction Act (PL96-511), 1980 [PRA80] - Defines the process to reduce paperwork and enhance the economy and efficiency of the Government and private sector by improving Federal information policy-making.

7. Federal Managers' Financial Integrity Act (PL97-255), 1982 [FMFIA82] - Requires that agency internal control systems be periodically evaluated and that the heads of executive agencies report annually on their systems' status.

8. Standards for Internal Controls in the Federal Government, by U.S. General Accounting Office, 1983 [GA083] - Presents the internal control standards to be fol-

lowed by executive agencies, covering both the program management as well as the traditional financial management areas.

9. OMB Circular A-123, 1981 [OMB123] & A-123R, 1983 [OMBR123] - Prescribes the policies and standards to be followed by executive agencies in establishing and maintaining internal controls in their programs and administrative activities.

10. OMB Circular A-127, 1984 [OMB127] - Prescribes policies and procedures to be followed by executive agencies in developing, operating, evaluating, and reporting on financial management systems.

11. OMB Circular A-130, 1985 [OMB130] - Establishes policy for the management of Federal information resources as well as procedures for information system security.

1.2 RISKS GENERATED BY COMPUTER TECHNOLOGY

1.2.1 Overview of Risks

Organizations assume risks in the conduct of their activities. These risks represent potential damaging events occurring that can produce losses. Controls or safeguards are installed to reduce these risks. If controls are insufficient, specific opportunities for loss remain which are too large.

The two elements that generate the risks in a computerized environment are its unique vulnerabilities and its unique set of threats. A vulnerability is a weakness or flaw in a computer-based system that may be exploited by a threat to cause destruction or misuse of its assets or resources. Threats can be physical (e.g., fire, water damage, earthquakes, and hurricanes) or people-oriented (e.g., errors, omissions, intentional acts of violence, and fraud). When a threat materializes and takes advantage of a system's vulnerabilities, a damaging event occurs that causes a loss. The risk of damaging events cannot be totally eliminated, but the use of controls on vulnerabilities and/or threats can reduce such risks to an acceptable level.

The purposes of a risk analysis of a computerized environment are (1) to search out its vulnerabilities and the probabilities of threats materializing to exploit these vulnerabilities, and (2) to calculate the damage or loss to its assets that could be produced by the resulting damaging events.[5] Auditors should assess a computerized environment's vulnerabilities and

5 There is no consensus on the definition of risk analysis. Some people add a third component, "to make control or safeguard recommendations that will reduce the damages or loss to an acceptable level, through the use of a cost/benefit analysis." Others in the field, however, consider that this addition makes the activity a risk management program.

set of threats to arrive at some estimate of possible damaging events. Such an assessment would also necessarily include reviewing the strength of existing controls.

1.2.1.1 Definitions - Some useful definitions in the context of computer security and audit follow. Appendix C contains definitions of additional relevant terms as well as the following.

1. Vulnerability: A vulnerability is a design, implementation, or operations flaw that may be exploited by a threat, to cause the computer system or application to operate in a fashion different from its published specifications and to result in destruction or misuse of equipment or data [NBS SP 500-57, p.A-2].

2. Vulnerability assessment: The process of (1) identifying flaws and the controls associated with those flaws in order to evaluate the adequacy of the control to reduce the risks to an acceptable level, and (2) identifying those flaws requiring management action, where risks are found to be too high.

3. Computer Generated Risk: Computer generated risk is the potential loss or damage to an organization that results from the use or misuse of its computer [adapted from NBS SP 500-57, p. A-2]. This may involve unauthorized disclosure, unauthorized modification, and/or loss of information resources as well as the authorized but incorrect use of a computer. Risk can be measured to some extent by performing a risk analysis.

4. Risk analysis: Risk analysis is an analysis of an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities [NBS SP 500-57, p. A-3]. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage to assets or resources in terms of dollars or other assets.

1.2.1.2 Vulnerability/Risk Related Requirements - Government-wide mandates/directives as well as agency-specific regulations require Federal agencies to conduct vulnerability assessments. These requirements are found in OMB Circulars A-123, A-127, and A-130. A vulnerability assessment is conducted using part of a risk analysis. The vulnerability assessment is a major assessment of the adequacy of an agency's controls and uses many tools to accomplish it, e.g., risk analysis. The Federal agencies must first identify vulnerabilities and threats, and then determine whether controls are adequate to reduce the resulting risks to an acceptable level. If not, vulnerabilities will have been identified which need to be corrected, and threats will have been identified which need to be guarded against by those Federal agencies.

1.2.2 Risks in a Computerized Environment

The risks in a computerized environment include both the risks that would be present in manual processing, plus some risks that are unique or increased in a computerized environment. The auditor should identify these risks, estimate the severity of the risks, and then develop audit tests to substantiate the impact of the risks on the application. For example, if the auditor felt that erroneous processing was a very high risk for a specific application, then the auditor should devise tests to substantiate the correctness or incorrectness of processing. This could be accomplished in a variety of ways. One way to verify processing accuracy would be to use Computer Assisted Audit Techniques (CAATs).

1.2.2.1 Additional Risks Present in a Computerized Environment - The use of a computer introduces additional risks into the system environment. Thus, besides the traditional risks, the auditor needs to assess the impact of these additional risks. The auditor should be aware of these special risks because they pose threats which are not present at all or are present to a lesser degree in non-computerized environments.

These additional risks include problems associated with:

- Improper use of technology;
- Inability to control technology;
- Inability to translate user needs into technical requirements;
- Illogical processing;
- Inability to react quickly;
- Cascading of errors;
- Repetition of errors;
- Incorrect entry of data;
- Concentration of data;
- Inability to substantiate processing; and
- Concentration of responsibilities.

Each of these risks is discussed individually in Appendix D, including many of the conditions that cause the risks to occur.

1.2.2.2 Assessing Vulnerabilities Through the Audit Process - The objective of control is to reduce risk. In an ideal environment, everything would be processed correctly, and there would be no need for control. Unfortunately, that environment does not exist, and risks are present which may introduce damaging events into the processing environment. Controls reduce the number and/or severity of damaging events to an acceptable level.

In order to evaluate the effectiveness of controls, the auditor must determine the vulnerabilities present in the computerized environment and the resulting risks. Until the risks are understood, the effectiveness of controls in reducing those risks cannot be evaluated. Thus, if the auditor is going to place reliance on controls, the auditor must both identify the vulnerabilities and determine the severity of those risks in the operating environment. It will be useful for auditors, as they consider application system and data file risks, to be aware of the many undesirable events which can have serious consequences.

The National Bureau of Standards' FIPS PUB 65 [FIPS65] provides the auditor and systems developer a list of negative situations to which application systems are vulnerable, grouped according to common system organizational structures. Those vulnerability lists are reprinted in Appendix E of this guide for the reader's convenience. While they are not intended to be all inclusive, they are suggestive of the various kinds of vulnerabilities that may exist in every system.

The list of potential vulnerabilities helps identify the additional risks in a computerized environment. Due to their value to the ADP auditor, as a tool in the identification of unique risks, a brief description of the types of vulnerabilities found in FIPS PUB 65 is repeated below.

1. Erroneous or Falsified Data Input - Erroneous or falsified input data is the simplest and most common cause of undesirable performance by an applications system. Vulnerabilities occur wherever data is collected, manually processed, or prepared for entry to the computer.

2. Misuse by Authorized End Users - End users are the people who are served by the ADP system. The system is designed for their use, but they can also misuse it for undesirable purposes. It is often very difficult to determine whether their use of the system is in accordance with the legitimate performance of their job.

3. Uncontrolled System Access - Organizations expose themselves to unnecessary risk if they fail to establish controls over who can enter the ADP area, who can

use the ADP system, and who can access the information contained in the system.

4. Ineffective Security Practices for the Application - Inadequate manual checks and controls to ensure correct processing by the ADP system, or negligence by those responsible for carrying out these checks, result in many vulnerabilities.

5. Procedural Errors Within the ADP Facility - Both errors and intentional acts committed by the ADP operations staff may result in improper operational procedures, lapsed controls, and losses in storage media and output.

6. Program Errors - Applications programs should be developed in an environment that requires and supports complete, correct, and consistent program design, good programming practices, adequate testing, review, and documentation, and proper maintenance procedures. Although programs developed in such an environment may still contain undetected errors, programs not developed in this manner will probably be rife with errors. Additionally, programmers can deliberately modify programs to produce undesirable side effects or they can misuse the programs they are in charge of.

7. Operating System Flaws - Design and implementation errors, system generation and maintenance problems, and deliberate penetrations resulting in modifications to the operating system can produce undesirable effects in the application system. Flaws in the operating system are often difficult to prevent and detect.

8. Communications System Failure - Information being routed from one location to another over communication lines is vulnerable to accidental failures and to intentional interception and modification by unauthorized parties.

Both management and auditors conduct vulnerability assessments. Management does the review as required by OMB Circular A-123, while the auditor does it as an independent assessment. The auditor looks both at management's performance of the review and at tests for inadequacies in management's system of internal controls.

1.3 CONTROL OBJECTIVES AND STANDARDS IN A COMPUTER ENVIRONMENT

1.3.1 Impact of the Computer on Controls

The objectives of control do not change in a computerized environment. The control objectives that are applicable to a manual system are equally applicable to a computerized system. What changes are the control techniques used to achieve the control objectives.

The new control complexities introduced by the computer require that, in addition to controlling the traditional processes, new control techniques be introduced. These would cover the automated processes themselves, as well as the interface between the manual and automated processes (an area where control problems often occur).

Examples of the new types of controls that exist within the computer processes include controls to ensure that:

- Proper versions of programs are in operation;
- Data integrity is maintained as it is passed between programs; and
- Access to the system is limited to only authorized individuals.

Examples of the new types of controls introduced as a result of the interface between the manual and automated processes include controls to ensure that:

- All data to be entered for computer processing is, in fact, input for processing;
- Only correctly entered data is accepted for computer processing; and
- Rejected data is maintained on an automated suspense file until corrected.

Thus, new control techniques must be used to reduce the new, unique risks introduced by the computerized environment.

1.3.2 Internal Control and Computer Security Review Policy

The U.S. General Accounting Office (GAO), as required by the Federal Managers' Financial Integrity Act of 1982 [FMFIA82], has defined the internal control standards [GAO83,p. 9] to be followed by executive agencies in establishing and maintaining systems of internal control. This GAO document on internal control standards provides guidance for agencies in developing systems of internal control for AISs. It is through those control systems that Federal managers fulfill their control responsibilities.

The purpose of systems of internal control is to reasonably ensure that the following goals are achieved:

1. Obligations and cost comply with applicable law.

2. All assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

3. Revenues and expenditures applicable to agency operations are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and accountability of these assets may be maintained.

The Federal Managers' Financial Integrity Act directs the heads of executive agencies to conduct annual evaluations of their internal control systems using guidelines established by the Office of Management and Budget. These guidelines are incorporated into the audit programs included in later sections of this manual. Controls not built into systems under development will probably not be added in the operational system. As has been discussed earlier in Section 1.1.4.3, modification of operational systems is extremely difficult and costly. Excessive cost and programmatic requirements frequently prohibit building controls into systems once operational.

The Comptroller General has defined the minimal level of quality acceptable for internal control systems in operation [GAO83]. They constitute the criteria against which systems of internal control are to be evaluated in the Federal government. The minimum level of internal control is divided into the following three categories:

1. General standards

   (a) Reasonable assurance: Internal control systems are to provide reasonable assurance that the objectives of the systems will be accomplished.

   (b) Supportive attitude: Managers and employees are to maintain and demonstrate a positive and supportive attitude toward internal controls at all times.

   (c) Competent personnel: Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

   (d) Control objectives: Internal control objectives are to be identified or developed for each agency activity and are to be logical, applicable, and reasonably complete.

   (e) Control techniques: Internal control techniques are to be effective and efficient in accomplishing their internal control objectives.

2. Specific standards

(a) Documentation: Internal control systems and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.

(b) Recording of transactions and events: Transactions and other significant events are to be promptly recorded and properly classified.

(c) Execution of transactions and events: Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.

(d) Separation of duties: Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

(e) Supervision: Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

(f) Access to and accountability for resources: Access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. Periodic comparison shall be made between the resources and the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

3. Audit resolution standard

When auditors identify potential control weaknesses, managers are required to promptly resolve these audit findings. Specifically, managers are to:

(a) Promptly evaluate findings and recommendations reported by auditors.

(b) Determine proper actions in response to audit findings and recommendations.

(c) Complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

The audit resolution standard requires managers to take prompt, responsive action on all findings and recommendations made by auditors. A responsive action is one which corrects identified deficiencies. Where audit findings identify opportunities for improvement rather than merely cite deficiencies, responsive action is considered to be that which produces improvements. The audit resolution process begins when the results of an audit are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the audit findings and recommendations are either invalid or do not warrant management action.

Auditors are responsible for following up on audit findings and recommendations to ascertain that resolution has been achieved. Auditors' findings and recommendations should be monitored through the resolution and follow-up processes. Top management should be kept informed through periodic reports so it can assure the quality and timeliness of individual resolution decisions.

1.4 EVIDENCE IN AUTOMATED SYSTEMS

The evidence collected to support findings in an automated system may differ drastically from traditional audit evidence. For example:

1. Transactions might be entered with no hard-copy equivalent. The "evidence" might have to be obtained from a data base management system.

2. Authorizations might be entirely electronic, through use of a password, with no written signature available to examine.

3. Procedures might not be found in a written manual but rather in coded instructions in a program which directs operations through terminal screen prompts or instructions.

4. The audit trail which supports a transaction process in an automated system, is itself automated. Rather than a paper trail, the trail might reside on computer tapes or disk files or other electronic media.

In Appendix F, other changes in audit evidence are enumerated along with three brief examples describing where evidence changed due to automation. Auditors must anticipate evidence needed during AIS development to insure proper consideration is given to related controls.

1.5 AIS AUDITABILITY

Auditability should be a management concern and relates to management control responsibilities. Auditability relates to the substantial evidential matter produced and retained by AISs, and the ability to locate and reconstruct processing. Auditability also encompasses the system of internal controls which assures the integrity of processing and the protection of evidential matter.

Auditability takes on greater importance in AISs because many of these systems have eliminated the traditional source documents. Transactions are originated electronically, and thus auditability is dependent upon the ability of the system to substantiate the integrity of those input transactions. This integrity is assured through an adequate system of internal controls.

The concept of auditability requires audit involvement in the development of AISs. Retrofitting controls in AISs is expensive and difficult on an after-the-fact basis. Therefore, the auditability and effective controls allowing for managerial and audit oversight must be designed and incorporated into AISs as those systems are developed.

CHAPTER 2
AIS LIFE CYCLE CONSIDERATIONS

2.1 BACKGROUND

2.1.1 PCIE - EDP Systems Review and Security Work Group

In October 1983, the President's Council on Integrity and Efficiency (PCIE) established a working group on Electronic Data Processing (EDP) Systems Review and Security[6] under the leadership of the Inspector General of the Department of Health and Human Services. Included under the umbrella of the Computer Security Project, the Work Group was charged with exploring ways to facilitate and improve Office of Inspector General reviews of automated information systems (AISs), particularly those systems under development. Its objective was to improve the likelihood that auditable and properly controlled systems are developed. While the Work Group looked at automated systems throughout the entire system life cycle (SLC), the clear focus was on the system development life cycle (SDLC) and the auditor's role in that process.

2.1.2 System Development Life Cycle

While the concept of a SDLC is not a new one, linking it and the generally accepted phase activities to other AIS and Information Resources Management (IRM) standards and requirements has not heretofore been successfully accomplished. Similarly, despite the growth of ADP audit units in the OIGs, and recognition of the significant benefits to be gained from proactive reviews (i.e., those conducted during the system development process), few developmental audits have been conducted. One of the key deterrents appears to be the confusion that exists regarding the actual role of the auditor during the SDLC.

To achieve their objective, and to clarify the role of the OIG/auditor, the PCIE Work Group drew upon the Department of Defense life cycle approach to the management of automated systems and the National Bureau of Standards/Institute for Computer Sciences and Technology's Federal Information Processing Standards Publications (FIPS PUBS) and Special Publications. Using this information, the Work Group developed an SLC functional matrix for AISs. The matrix, structured around critical AIS documentation requirements, is intended to clarify the functions of the auditor vis-a-vis other key participants in the ADP planning, design, implementation, and review processes. With the matrix as a conceptual framework, this audit guide is intended to facilitate the successful fulfillment of that role, focusing on systems under development and major modifications to existing systems.

---

6 See Appendix A for more information on the activities of this group.

2.2 OPERATING ENVIRONMENT

The AIS life cycle used to develop systems will not be the same in every agency. In addition, the operating environment for the life cycle is a function of the agency in which it exists and also varies from agency to agency. There is no single standard SDLC for the Federal government. This chapter describes good practice for the SDLC and its operating environment. The use by Federal agencies of these AIS life cycle practices should result in a well-controlled and auditable AIS.

Management establishes the environment in which systems are developed. If the environment is structured, the probability of a well-defined life cycle and compliance to it increases. A loose management style leads to free-form system development which may result in serious omissions. The operating environment reflects the adequacy of the general controls over system development, operations, and maintenance.

2.2.1 IRM Planning and Implementation of Policy Guidelines

Agencies need to perform overall long-range IRM planning. The purpose of this planning is to determine which AIS projects are to be implemented, the priority and schedule for their implementation, the individual(s) responsible for implementation, and the amount of resources to be allocated to each project.

In addition to formal IRM planning, organizations must identify and follow policies/procedures/standards for developing AISs. These policies/procedures/standards should be established and promulgated within the organization, based on guidance provided by such agencies as the National Bureau of Standards and the General Services Administration.

Each of these two major considerations is discussed in some detail below.

2.2.1.1 IRM Planning - IRM planning is a means of selecting, prioritizing, budgeting, and assigning projects to individuals and groups to implement. Many organizations have adopted the concept using a management steering committee, an IRM planning committee, or an executive IRM committee.

The following are the desirable characteristics of such an IRM planning committee:

(a) Is comprised of senior managers - The IRM committee should be chaired by the senior manager of the agency, and be comprised of the direct subordinates of that senior manager.

(b) Has representatives from all major agency data users - It is important that all users of information processing services are represented on the IRM committee. This committee will establish priorities of work, which require that all users of ADP services have a voice in how those resources are allocated. In addition, users such as budgeting, legal, and ADP audit should also be represented on the IRM committee.

(c) Meets on a regular basis - For most agencies, quarterly is sufficient.

(d) Establishes AIS implementation priorities - The IRM committee determines which systems are implemented, and in what sequence. Note that the IRM committee may also determine other data processing priorities, such as implementation of major software packages (e.g., data base management systems).

(e) Identifies and assigns projects to a Sponsor - The Sponsor is the individual responsible for implementing the AIS. For many systems, multiple entities will be involved. Thus, it is important for the IRM committee to identify who is in charge, and then ensure that that individual has adequate resources at his/her disposal to successfully implement the project.

(f) Monitors status of projects - The IRM committee must retain responsibility for projects, and therefore should be receiving regular status reports on approved AIS projects. If projects fall behind schedule, or encounter other problems, the IRM committee should take appropriate action.

2.2.1.2 Using Policy/Procedures/Standards - Although there is no uniform SDLC for the Federal government, there are a variety of policies, procedures, and standards which have been issued relating to the development of AISs. Many of these have been issued by the National Bureau of Standards, the General Services Administration's Office of Software Development, the Office of Management and Budget (OMB), and the U.S. General Accounting Office (GAO). The objective of these policies/procedures/standards is to increase the probability of success for the AIS.

Some of the more pertinent publications that system development projects should follow are listed below and can be found in Appendix G and H (annotated with an asterisk). Auditors involved in the system development process should study these publications to ensure that they follow the guidance.

2.2.1.2.1 References Used by the Life Cycle Matrix - The following references are cited in the Life Cycle Matrix in Figure 1.

1. FIPSPUB38 GUIDELINES FOR DOCUMENTATION OF COMPUTER PROGRAMS AND AUTOMATED DATA SYSTEMS, 1976 February 15 [FIPS38].

Provides basic guidance for the preparation of ten document types that are used in the development of computer software. Can be used as a checklist for the planning and evaluation of software documentation practices.

2. FIPSPUB 64 GUIDELINES FOR DOCUMENTATION OF COMPUTER PROGRAMS AND AUTOMATED DATA SYSTEMS FOR THE INITIATION PHASE, 1979 August 1 [FIPS64].

Provides guidance in determining the content and extent of documentation needed for initiation phase of the software life cycle. Covers preparation of project requests, feasibility studies, and cost/benefit analysis documents.

3. FIPSPUB 65 GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS, 1979 August 1 [FIPS65].

Presents a technique for conducting a risk analysis on an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of occurrence and the damage caused by adverse events.

4. FIPSPUB 73 GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS, 1980 June 30 [FIPS73].

Describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing, and operating computer systems which require protection.

5. FIPSPUB 101 GUIDELINE FOR LIFECYCLE VALIDATION, VERIFICATION, AND TESTING OF COMPUTER SOFTWARE, 1983 June 6 [FIPS101].

Presents an integrated approach to validation, verification, and testing (VV&T) that should be used throughout the software lifecycle. Also included is a glossary of technical terms and a list of supporting NBS publications. An appendix provides an outline for formulating a VV&T plan.

6. FIPSPUB 102 GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION, 1983 September 27 [FIPS102].

Describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authori zation for the operation of the system and is based on the certification process. Also included is a glossary of terms.

7. FIPSPUB 105 GUIDELINE FOR SOFTWARE DOCUMENTATION MANAGEMENT, 1984 June 6 [FIPS105].

Provides explicit advice on managing the planning, development, and production of computer software documentation. Includes several checklists, references to relevant standards and guidelines, and a glossary of terms.

8. NBS SPEC PUB 500-98 PLANNING FOR SOFTWARE VALIDATION, VERIFICATION, AND TESTING, Patricia B. Powell, Editor, November 1982 [NBS98].

Presents a guide for managers, programmers, and analysts to aid in developing plans for software VV&T and in selecting appropriate practices, techniques, and tools. In explaining the fundamental concepts, this report provides information to help in establishing organizational policies for VV&T.

9. NBS SPEC PUB 500-105 GUIDE TO SOFTWARE CONVERSION MANAGEMENT, Mark Skall, Editor, October 1983 [NBS105].

Describes explicit steps for carrying out software conversion projects. This guide was developed to help managers avoid the common problems associated with software conversion. It includes an extensive reference list, case studies, and a glossary of terms.

10. DOD7920.2 MAJOR AIS APPROVAL PROCESS, DOD INSTRUCTION, October 20, 1978 [DOD78-2].

Establishes the review and decision process and procedures for the development of major AISs. It implements DOD's life cycle management directive 7920.1.

2.2.1.2.2 Major GSA References - The following are major references by GSA on this subject area. Other GSA references can be found in Appendices G and H. Also cited in Appendix G are the definitions of four classes of GSA regulations that are pertinent to this subject area.

1. SOFTWARE IMPROVEMENT - A NEEDED PROCESS IN THE FEDERAL GOVERNMENT, June 1981 [GSA81-1].

   An easy-to-read introduction to the concepts of software improvement and how these concepts can be used to effectively modernize Government software.

2. GUIDELINES FOR PLANNING AND IMPLEMENTING A SOFTWARE IMPROVEMENT PROGRAM (SIP), May 1983 [GSA83-3].

   Serves as a starting point for establishing, planning, and implementing a SIP. Emphasizes the top-down incremental approach to software improvement and explains what needs to be done to set up a SIP in an organization.

3. THE SOFTWARE IMPROVEMENT PROCESS--ITS PHASES AND TASKS (PARTS 1 & 2), July 1983 [GSA83-5].

   A companion for the "Guidelines" described above, this report goes into greater detail discussing the phases and tasks needed for planning and implementing a SIP.

4. ESTABLISHING A SOFTWARE ENGINEERING TECHNOLOGY (SET), June 1983 [GSA83-4].

   Software engineering is an approach to managing software development and maintenance by using standards, procedures, and automated tools. This book serves as a starting point for implementing a SET in your organization.

2.2.2 AIS Development Methodologies

In the past, few structural restrictions were placed on the system designer. The project team was given a mission and resources to accomplish that mission. The methods they chose for building the AIS were left to their discretion. As a result, many systems were installed late, followed no standards, were significantly over budget, and often failed to meet user needs.

This unstructured design approach offered minimal opportunities for management, let alone the auditor, to identify problems during development. It was not until installation that problems became apparent. The solution to this management dilemma was to develop a for-

malized method for developing automated systems. These methodologies are alternately called system development methodologies (SDMs), system development life cycle (SDLC), or system life cycle (SLC) methodologies.

The following are generally accepted as the desirable practices of a good SDLC methodology:

1. Predefined documents/deliverables - All of the products/deliverables to be developed during the creation of an automated system need to be defined. In the better design methodologies, these products/documents are standardized. They will either be preprinted forms, or screens available to the designer on computer terminals. The sequence in which the products are created is also determined. In most instances, the output from one product or set of products is needed before the next product can be developed.

2. Life cycle phases or checkpoints - The life cycle should be divided into segments defined by activities and outcomes or deliverables. Each segment encompasses some part of the developmental process. The purpose of having distinct phases or checkpoints is to allow decisions to be made regarding completion of the project, changes in direction, cancellation of the project, and authorization for use of more resources on the project at these points in time. Note that management in many organizations only authorizes work (i.e., resources) on an AIS project through the next management checkpoint. This is done to assure that management can continually evaluate project status and make the appropriate management decisions.

3. Completion of products/documents are tied to life cycle phase checkpoints - At each checkpoint, specified work is to be completed. This work is normally expressed as documents to be produced. Thus, when someone reviews a project at a checkpoint they know which products/documents are to be delivered at that point in time. This also helps ensure that the project is on schedule and within budget. It is through the examination of these products that the status of work can be determined.

4. Reviews are product/document reviews - Reviews of the status of projects are performed by reviewing the products/documents produced by the project team. Therefore, it is important that these products/documents be produced in a standardized format. The National Bureau of Standards, through its various FIPS publications, has issued standards for most of the documents produced during the developmental process [FIPS38, FIPS64]. These reviews must be signed off on upon completion, indicating satisfactory completion of the product/document, and life cycle phase.

5. Training is tied to products/documents - The training program for people associated with developmental projects is centered around the products/documents to be produced. Auditors involved in the developmental process should become familiar with the developmen-

tal products/documents in order to properly review that project. While the auditor need not know how to develop the products, the auditor should understand the meaning of the information contained in those documents, and how the documents tie together in the organization's SDLC process.

2.2.3 Project Administration and Control

Project administration and control are the tools of management to monitor and direct the project during implementation. The life cycle methodology, and the developmental products, are designed to create a secure, accurate, and cost-effective system to meet user needs. Project administration and control produce documents which are used by management in administering the project. The developmental products are normally retained as part of the system documentation and become input to maintenance of the system. Project administration and control documents generally have a limited life, and are not retained for the life of the system but through the SDLC.

The project administration and control documents can be used by the auditor to evaluate the status of projects and to evaluate the performance of project management. Project status is evaluated by the products that relate actual work to scheduled/budgeted work. Project management is evaluated on its ability to produce the specified work products in accordance with the project management plan.

The products/documents used for project administration and control include:

1. Budgeting/budget status reports - The funds allocated for development of AISs and the internal budgetary reporting systems stating the use of funds against budgets.

2. Scheduling/schedule status reports - The division of system development tasks into phases/deliverables, and relating those phases/deliverables to specific time frames. The status report indicates whether or not the deliverables have been accomplished within the stated time frames.

3. Development project status reports - Reports prepared by the individual project members indicating the status of deliverables under their responsibility. To be effective, these status reports must be able to definitively state the percent of work done, as opposed to the amount of resources consumed.

4. Checkpoint review status report - The results of a formal analysis by which an independent group evaluates the completeness of work or product deliverables at specific system development checkpoints.

5. Resource utilization report - Status reports produced by computer operations. These reports are normally generated automatically from statistical information collected about resources consumed during the development project. One such package is IBM's job accounting system called System Management Facility (SMF).

6. Project management software system - Organizations utilize a variety of management software systems to control projects. A commonly used software package is PAC II, which is a scheduling and status reporting system.

7. Automated software development environments -Complete and self-contained software development, documentation, and test tools and techniques for systems analysts, programmers, and reviewers. In general, such environments will automatically generate all the reports and code, and provide mapping back to high level specifications.

In most AIS projects, more emphasis is placed on system development than project management. Thus, the auditor is more apt to find well-defined developmental products than to find well-developed project administration and control documents. Many of the administrative documents are more quantitative in nature (e.g., stating the amount of resources used) as opposed to qualitative in nature (e.g., indicating percentage of project completion in relation to the developmental work products).

2.2.4 AIS Life Cycle Matrix

Auditors cannot comprehensively review a system under development until there is some structure to the development process. Without structure, the auditor will be unable to determine what deliverables are to be produced at what time. On the other hand, it is recognized that different agencies within the Federal government use different system development methodologies.

As a basis for structuring the review proposed by this guide, the PCIE Work Group on EDP Systems Review and Security[7] defined a recommended AIS life cycle process in the form of a Life Cycle Matrix (see Figure 1). This life cycle matrix was developed based on the more

7 See Appendix A for a description of the PCIE Work Group and its efforts in producing this life cycle matrix.

PART		VI INSTALLATION & OPERATION
POLICY / OVERSIGHT	Inform ance Offical hd	● approves final installation of system; accredits all systems determined to be of critical sensitivity or importance to the Dept.; directs periodic reviews per P.L. 96-511 for continued need
	System eport Contro &	● conducts periodic reviews per OMB Circulars A-123, A-127, and A-130; feeding into long-range AIS planning process
	Audito stalla- curity	● conducts periodic reviews per OMB A-130 & GAO audit standards; updates Audit Plan and Program as needed
FUNCTIONAL / OPERATIONAL	Sponso Con- er- ation	● oversees training; directs periodic reviews of sensitive applications for recertification; identifies need for changes to system and revises Project Plan accordingly
	Project Techni tem Plan	● directs implementation and updates User Manual & Operations/Maintenance Manual as needed during implementation and operation
	System d Special er stal-	● conducts periodic reviews per OMB Circulars A-123, A-127, and A-130
	Contra	● if appropriate, continues to assure contract compliance
	ADP N al. n- ical	● conducts periodic reviews per OMB Circular A-130; provides technical assistance; maintains system documentation
	Quality ad- ent	● reviews changes to software system; summarizes, analyzes and reports on defects to responsible participants

hin the phase or

Figure 1. AUTOMATED INFORMATION SYSTEM (AIS) - LIFE-CYCLE MATRIX [1]

PARTICIPANTS \ LIFE-CYCLE PHASES		DEVELOPMENT					
	OPERATING ENVIRONMENT	I INITIATION	II DEFINITION	III SYSTEM DESIGN	IV PROGRAMMING & TRAINING	V EVALUATION & ACCEPTANCE	VI INSTALLATION & OPERATION
POLICY / OVERSIGHT — Information Resources Management (IRM) Offical [2]	• establishes system life-cycle principles, documentation requirements, records management policy, & long- range system planning and decision process; with OIG establishes procedures by which OIG is notified of all significant new systems or systems modifications	• approves Needs Statement	• approves System Decision Paper to advance to Phase II, in consultation with Sponser/User and ADP Manager (occurs between Phases) [3]	• approves updated System Decision Paper to advance to Phase III, in consultation with Sponsor/User and ADP Manager (occurs between Phases), & enters system into Dept's. formal systems' inventory	• approves updated System Decision Paper to advanceto Phase IV, in consultation with Sponsor/User and ADP Manager (occurs between Phases)	• approves updated System Decision Paper to advance to Phase V, in consultation with Sponsor/User and ADP Manager (occurs between Phases)	• approves final installation of system; accredits all systems determined to be of entical sensitivity or importance to the Dept.; directs periodic reviews per P.L. 96-511 for continued need
POLICY / OVERSIGHT — System Security Officer (SSO)/Internal Control Officer (ICO)	• establishes Dept. internal control and computer security policy, per OMB Circulars A-123, A-127, & A-130; also develops policy pertaining to privacy requirements of agency records and data, per Privacy Act of 1974	• oversees or conducts Risk Analysis; helps to evaluate system sensitivity	• reviews SSO/ICO components of Project Plan, Functional Requirements Documents & Data Requirements Documents, on a select basis	• reviews SSO/ICO components of System/Subsystem, Program and Data Base Specifications, and Validation, Verification and Testing Plan and Specifications	• reviews SSO/ICO components of User Manual, Operations/Maintenance Manual, Installation and Conversion Plan, and revised VV&T Plan and Specifications	• reviews Test Analysis and Security Evaluation Report and SSO/ICO components of revised Installation & Conversion Plan	• conducts periodic reviews per OMB Circulars A-123, A-127, and A-130; feeding into long-range AIS planning process
POLICY / OVERSIGHT — Auditor (OIG)	• develops ADP audit guide; conducts selective reviews or audits of automated systems, based on established criteria for prioritizing systems, and reports on needed management improvements [4]	• reviews/evaluates Needs Statement, Feasibility Study, Risk Analysis, Cost/Benefit Analysis, and System Decision Paper; based upon review determines scope of future involvement	• reviews/evaluates System Decision Paper, Project Plan, Functional Requirements Documents, Data Requirements Documents, and participates in their development, as necessary; prepares Audit Program	• reviews/evaluates & possibly inputs to Risk Analysis, Sys. Decision Paper, Sys./Subsys Program & Data Base Specs., VV&T Plan and Specs. and Revised Project Plan; updates Audit Program	• reviews/evaluates revised Project Plan, System Decision Paper, revised VV&T Plan and Specifications,User Manual, Operations/Maintenance Manual, and Installation & Conversion Plan; updates/Audit Program	• reviews/evaluates revised Project Plan, revised Installation & Conversion Plan, and Test Analysis & Security Evaluation Report; updates Audit Program	• conducts periodic reviews per OMB A-130 & GAO audit standards; updates Audit Plan and Program as needed
FUNCTIONAL / OPERATIONAL — Sponsor/User	• establishes management level implementation guidelines & approval process for AISs; organizes a formal quality assurance function to provide for internal management reviews & recommendations pertaining to ADP efforts	• identifies & validates need; develops Needs Statement; directs Feasibility Study, Risk Analysis, and Cost/Benefit Analysis; develops System Decision Paper; selects a Project Manager	• approves Project Plan and Functional Requirements Documents, and updates System Decision Paper	• approves revised Project Plan and updates System Decision Paper; reassesses Risk Analysis; approves Validation, Verification and Testing Plan and Specifications (all based on QA recomendations)	• approves revised Project Plan, revised VV&T Plan and Specifications, User Manual, Operations/Maintenance Manual & Installation & Conversion Plan; updates System Decision Paper; initiates user training	• approves revised Project Plan and Installation & Conversion Plan; updates System Decision Paper; oversees training; accepts (accredits) system for operation	• oversees training; directs periodic reviews of sensitive applications for recertification; identifies need for changes to system and revises Project Plan accordingly
FUNCTIONAL / OPERATIONAL — Project Manager (PM)/Contracting Officer's Technical Representative (COTR) [5]	• N/A	• develops or oversees development of Feasibility Study, Risk Analysis, Cost/Benefit Analysis, and System Decision Paper	• develops Project Plan and Functional and Data Requirements Documents with User participation	• updates Project Plan; develops System/Subsystem Program & Data Base Specifications, & Validation, Verification and Testing Plan and Specifications	• updates Project Plan, revises VV&T Plan and Specifications; develops User Manual, Operations/Maintenance Manual, and Installation & Conversion Plan; responsible for programming and testing	• updates Project Plan; supports & oversees Test Analysis & Security Eval. Report and certifies system security; revises User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan based on test results	• directs implementation and updates User Manual & Operations/Maintenanre Manual as needed during implementation and operation
FUNCTIONAL / OPERATIONAL — System Security Specialist (SSS)/Internal Control Specialist (ICS)	• establishes policy implementation guidelines & planning processes for individual system development efforts, based on Dept., requirements and OMB Circulars A-123, A-127, & A-130 guidance	• conducts Risk Analysis as appropriate	• provides consultation & review of SSO/ICO components of Project Plan, Functional Requirements Documents and Data Requirenients Documents	• reviews SSO/ICO components of System/Subsystem, Program and Data Base Specifications, and Validation, Verification and Testing Plan and Specifications	• reviews SSO/ICO components of User Manual, Operations/Maintenance Manual, Installation & Conversion Plan, and revised VV&T and Specifications Plan	• reviews Test Analysis & Security Eval. Report and SSO/ICO impacted documentation updates to User Manual, Operations/Maintenanre Manual, and Installation and Conversion Plan	• conducts periodic reviews per OMB Circulars A-123, A-127, and A-130
FUNCTIONAL / OPERATIONAL — Contracting Offirer/Contract Auditor [6]	• establishes policy implementation guidelines based on GSA/Dept. procurement policy	• if appropriate, awards contract & assures contract compliance	• assures contract complianre	• same as Phase II	• same as Phase II	• same as Phase II	• if appropriate, continues to assure contract compliance
FUNCTIONAL / OPERATIONAL — ADP Manager	• establishes technical policy implementation guidelines for in-house application development, purchased software & contracted system development efforts	• provides consultation as appropriate, unless this office initiates system	• reviews Project Plan, Functional Req Doc's., Data Req. Doc's; as appropriate, provides technical support to Project Manager & Sponser/User	• reviews VV&T components of Sys./Subsys., Prog. & Data Base Specs., & VV&T Plan and Specs; as appropriate, provides technical support to Project Manager and Sponsor/User in developing Specs.	• reviews VV&T components of User Manual, Operations/Maintenance Manual and Installation & Conversion Plan; provides technical support to Project Manager and Sponsor/User; may conduct DP training	• directs tests; reviews Test Analysis & Security Eval. Report, and Installation and Conversion Plan; continues to provide technical support; may do technical evaluation for re tification.	• conducts periodic reviews per OMB Circular A-130; provides technical assistance; maintains system documentation
FUNCTIONAL / OPERATIONAL — Quality Assurance (QA) Specialist	• establishes and utilizes processes to insure applications systems meet requirements, including compliance with data processing procedures	• provides consultation on quality attributes of Needs Statement	• reviews project definition to ensure compliance with Needs Statement & data processing standards	• reviews system design, VV&T components and documentation for compliance to definition and data processing standards	• reviews program definition, program code, documentation, and training, for compliance to designand data processing standards	• reviews Test Analysis & Security Eval. Report and advises responsible participants on system achievement of Needs Statement	• reviews changes to software system; summarizes, analyzes and reports on defects to responsible participants

[1] Matrix intended to reflect, primarily, roles & documents for large, in-house AIS development or redesign efforts. Alternative approaches are discussed in body of report.
[2] IRM refers to "single offical" as identified under PL96-511 and OMB Circular A-130. For smaller systems, however, approval authorities commonly delegated, as provided for by Department policy.
[3] Relationship among IRM Official, Sponsor and ADP Manager may be formal, as in the case of an established AIS approval body, or informal ad hoc body, depending upon the organization and particular system.
[4] All audit involvement in AIS life cycle should be based on an assessment of need and potential risk/exposure, and performed on a select basis, not on all systems or phases.
[5] In some circumstances, some of these functions are handled by a COTR responsible to the Project Manager
[6] In some circumstances, some of these functions are handled by a Contract Auditor responsible to the Contracting Officer.

Key: The dot next to each entry in the matrix indicates whether that activity occurs within the phase or between two adjacent phases.

commonly recognized deliverables produced in Federal AIS projects, and a comprehensive survey of system development practices in over 100 offices of approximately 76 Federal agencies and in selected private sector companies. This life cycle matrix should be used by auditors as a basis for understanding how to review systems under development. Actual reviews must be tied to the particular development methodology used.

The AIS life cycle matrix is designed to be used by the auditor in the following manner:

1. As a training tool - The matrix defines the major phases in the development of an AIS in terms of key activities to be performed and products delivered. This matrix can be used to orient the auditor to the developmental process by explaining:

   (a) The phases/activities of the system development process;

   (b) The participants in the developmental process;

   (c) The responsibilities assigned to individual participants ("participants" refers to functional responsibilities for development rather than job titles or full-time positions); and

   (d) The products/deliverables to be produced.

2. As a basis for understanding a proposed review methodology - Because the specific development methodology of various Federal agencies may differ, it is only possible to provide a generalized audit review methodology. The framework for describing this methodology is the AIS life cycle matrix provided here.

3. For customization of the audit methodology to a specific Federal agency and AIS - The auditor may need to customize the review methodology in this guide to the specific AIS project under review. This can be accomplished by relating the deliverables/responsibilities in the agency to the AIS under review.

4. In the absence of having a formal methodology or using one, this matrix can be used by auditors as criteria for evaluating AISs under development.

2.3 LIFE CYCLE PHASES

The auditor should not expect that systems will be developed in accordance with this specific SDLC methodology. The life cycle phases described in this guide are intended to clarify the broad functions or activities which should occur during the development of an

automated system. The six phases cover activities commonly performed, so that whatever development methodology the auditor encounters, the following six phases encompass the activities likely to be found, and thus could be customized to a specific audit (see Figure 1, Automated Information System (AIS) - Life Cycle Matrix).

2.3.1 Initiation - Phase I

Consistent with the DOD "Mission Analysis" and "Concept Development" Phases, the initiation phase begins with the recognition of a problem and the identification of a need. During this phase, the need is validated, and the exploration of alternative functional concepts to satisfy the need is recommended and approved. The decision to pursue a solution must be based upon a clear understanding of the problem, a preliminary investigation of alternative solutions, including non-computer-based solutions, and a comparison of the expected benefits versus the cost (including design, construction, operation, and potential risks) of the solution. At this stage the risk/sensitivity of the data or information in or resources controlled by the AIS under consideration should be evaluated.

2.3.2 Definition - Phase II

In this phase, the functional requirements are defined, and detailed planning for the development of an operable AIS is begun. Functional requirements and processes to be automated are documented and approved by an appropriate senior management official before an AIS development effort is started. Requirements identification is iterative, as is the analysis of potential risk, and involves those who identify and solve problems. It is critical that internal control and specific security requirements be identified during this process. Requirements may be, and commonly are, modified in later phases as a better understanding of the problem is gained. Also, during Phase II, a Project Plan specifying a strategy for managing AIS development, certification, and accreditation is prepared. It defines the goals and activities for all subsequent phases, and includes resource estimates during each phase, intermediate milestones, as well as methods for design, documentation, problem reporting, and change control. Resource planning for VV&T should be included here [FIPS101]. In essence, the Project Plan describes the unique SDLC methodology to be used during the life of the particular project. During this phase, the Audit Plan is also prepared so that the new AIS will be auditable from the start.

2.3.3 System Design - Phase III

The activities performed during this phase result in a specification of the problem solution. The solution provides a specific high-level definition including information aggregates, information flows and logical processing steps, as well as all major interfaces and their inputs and outputs. The purpose is to refine, resolve deficiencies in, define additional details in, and

package the solution. The detailed design specifications describe the physical solution (algorithms and data structures) in such a way that it can be implemented in code with little or no need for additional analysis. Agencies should define and approve security specifications prior to acquiring or starting formal development of the applications. The validation, verification, and testing (VV&T) goals are also identified during this phase, and a plan for achieving these goals is developed (See National Bureau of Standards FIPS PUB 101). The Project Plan (schedules, budgets, deliverables, etc.) and Risk Analysis are reviewed and revised as required given the scope and complexity of the solution formulated. These activities are coordinated with the Certification Plan components.

2.3.4 Programming and Training - Phase IV

This phase results in programs which are ready for testing, evaluation, certification, and installation. Programming is the process of implementing the detailed design specifications into code. Completed code will then undergo unit testing, as described in the revised VV&T Plan in this phase, and integration and system testing in Phase V. In addition to Programming and Training Manuals, User and Maintenance Manuals are prepared during the fourth phase, as is a preliminary Installation Plan which specifies the approach to and details of the installation of the AIS.

2.3.5 Evaluation and Acceptance - Phase V

In this phase[8], integration and system testing of the AIS occurs. For validation purposes, the system should be executed on test data, and the AIS field tested in one or more representative operational sites. Using actual functional transaction data, if designated a "sensitive" system, the system should be certified for technical adequacy in meeting its security requirements by an appropriate authority, prior to accreditation and installation. Before certification, all VV&T test results would be documented and a comparison of actual and expected results made.

OMB Circular A-130 and NBS FIPS PUB 102 security evaluation should be part of the broader test results/test evaluation report. The accreditation statement, the last key activity of the phase, will be a statement from the responsible accrediting official (e.g., Sponsor/User)

---

8 Development Phase--The Institute for Computer Sciences and Technology at the National Bureau of Standards (ICST/NBS), in structuring a framework within which the development of software could be discussed, identified a Development Phase including four stages --definition, design, programming, and testing. These are represented by Phases II-V described above. During the Development Phase the requirements for software are determined and the software is then defined, specified, programmed, and tested. Documentation is prepared within this phase to provide an adequate record of the technical information developed. The PCIE Work Group's phases are intended to cover not only software but also hardware, telecommunications, etc., i.e., all the components of an automated information system

that the system is operating effectively and is ready to be installed. Any caveats or restrictions should be provided at this time.

2.3.6 Installation and Operation - Phase VI

Comparable to DOD's "Deployment and Operation" phase, and encompassing both NBS' "Installation" subphase and "Operation and Maintenance" phase, the purpose of this final life cycle phase is to: (a) implement the approved operational plan, including extension/installation at other sites; (b) continue approved operations; (c) budget adequately; and (d) control all changes and maintain/modify the AIS during its remaining life. Problem reporting, change requests, and other change control mechanisms are used to facilitate the systematic correction and evolution of the AIS. In addition, periodic performance measurement and evaluation activities are performed to ensure that the system continues to meet its requirements in a cost-effective manner in the context of a changing system environment. These reviews may be conducted by either or both the quality assurance (QA) staff or the audit unit.

2.4 RESPONSIBLE PARTICIPANTS AND THEIR FUNCTION IN THE AIS LIFE CYCLE

The auditor must recognize that organizational structures vary significantly from agency to agency. The functions described in this section are described as "job title related" functions so thatorganizations can look at them as specific job titles, if they have an equivalent job, or as functions which must be performed whether or not the specific job exists. The list is not meant to be all-inclusive, nor does it preclude smaller agencies or organizational units from combining participants or roles.

The rationale for describing the participants is to identify the role of each key participant. In the audit program, the auditor will be asked to verify that the respective AIS participants have each performed their appropriate role. A brief description of all of the participants listed in the AIS life cycle matrix follows, with the exception of the auditor, whose role constitutes the bulk of this guide and is found in Chapter 4. (Note that these functions are divided into policy/oversight participants and the functional/operational participants, based on the level of the agency at which they operate.[9])

2.4.1 Policy/Oversight Participants

2.4.1.1 Information Resources Management (IRM) Official - This individual is responsible for developing uniform policies and procedures to ensure that an agency effectively and

---

9 Policy/oversight participants tend to function at the department level, setting and/or overseeing implementation of internal control and security policy guidance. Functional/operational participants are located in program or line level and implement department policy or guidance

efficiently manages its records/information and its information resources. The IRM official is responsible for approving the development or acquisition of all information systems, though this responsibility may be shared with an approval body, or for some systems, delegated outside that position. The IRM function, that of a "single official," is called for in PL96-511 [PRA80] and in OMB Circular A-130 [OMB130].

2.4.1.2 System Security Officer (SSO) - At the department level, the SSO is responsible for the development, implementation, and operation of an agency's computer security program. Designated by the IRM official, that individual is expected to define and approve overall security specifications of new systems or changes to existing systems, whether developed in-house or acquired from an outside source. The SSO is also responsible for conducting or overseeing the conduct of risk analyses prior to the development of any major system. The function is identified in OMB Circular A-130.

2.4.1.3 Internal Control Officer (ICO) - At the department level, the ICO is responsible for seeing that an agency's financial management information systems are identified, developed, maintained, reviewed, and improved as necessary. The ICO is responsible for the conduct of vulnerability assessments of these financial management information systems, and their internal control points. The ICO responsibility is derived from OMB Circular A-123 [OMB123]. The ICO does not perform the reviews per se, but establishes policy for determination of the internal control points, and oversees the scheduling and conduct of reviews performed at the operational or program level.

2.4.2 Functional/Operational Participants

2.4.2.1 Sponsor/User - The Sponsor/User is responsible for initially identifying the need that has to be met by an AIS. The Sponsor/User has to identify various alternative solutions to the problem, and determine the feasibility and cost/benefit of the various alternatives. The Sponsor/User also has to conduct or oversee the conduct of a Risk Analysis, to assess the potential vulnerabilities of the system or application being developed. That analysis must be continually updated or revised during the SDLC to assure the inclusion of appropriate internal controls and security safeguards. The Sponsor/User is ultimately responsible for accepting (accrediting) the system as being complete, meeting its requirements, and being ready for operational use. Depending on the particular system, the Sponsor/User may be located at various levels in the agency. Under OMB Circular A-130, the Sponsor/User, as the official whose program an information system supports, should be responsible and accountable for the products of that system.

2.4.2.2 Project Manager/Contracting Officer's Technical Representative (COTR) - The Project Manager is the individual responsible for seeing that a system is properly designed to meet the Sponsor/User's needs, and is developed on schedule. The Project Manager is respon-

sible for seeing that all system documentation is prepared as the system is being developed. If the system is developed either in-house or by a contractor, the Project Manager is responsible for certifying that the delivered system meets all technical specifications, including security, obtaining technical assistance from the ADP Manager as necessary. If a different individual, the COTR should report to the Project Manager appraisals of technical adequacy of the AIS being developed by the contractor. The Project Manager is designated by the Sponsor or chief User and is responsible to the same.

2.4.2.3 System Security Specialist (SSS)[10] - This individual is responsible, at the program or operational level, for seeing that a system complies with the agency's computer/system security policy. The SSS approves design reviews, to assure that (1)the design meets approved security specifications and system tests, and (2)administrative, physical and technical requirements are adequate prior to installation of the system. The function is referenced in OMB Circular A-130, and must be coordinated with internal control review requirements under OMB A-123.

2.4.2.4 Internal Control Specialist- This individual is responsible, at the operational level, for seeing that a system complies with the agency's internal control policy. The ICS assures that a system meets basic standards for documentation, recording of transactions, execution of transactions, separation of duties, access to resources, and all other internal control requirements. The function is referenced in OMB Circular A-123, and should be coordinated with security review requirements under OMB Circular A-130.

2.4.2.5 Contracting Officer - The Contracting Officer is responsible for awarding and managing contracts to a vendor to provide part or all of the system development activity that is not performed by a unit within the operating agency. The contract might also provide for the procurement of system software required by a new application. The Contracting Officer in either case, is responsible for seeing that the vendor or contractor complies with the terms of the contract and that the deliverables are provided on time. Responsibilities are clearly stated in the existing regulations (i.e., FIRMR, FPMR, FAR and FPR). He/she works with the PM and COTR and, possibly, the Sponsor/User to assure that the request for proposal (RFP) and the final contract clearly reflects user needs and critical internal control and security features.

---

10 The title of System Security Specialist, or SSS, is used in place of System Security Officer (SSO) to differentiate the function and responsibility of the department's security office from that at the program or operational level. The same distinction applies to the Internal Control Specialist versus the Internal Control Officer.

(Contract Auditor - If requested by the Contracting Officer, the Contract Auditor is responsible for reviewing a contractor's performance on a specified contract. Otherwise, compliance with the contract would fall under the purview of the Auditor.)

2.4.2.6 ADP Manager - The ADP Manager is the technical individual responsible for the ADP installations and operations of an agency's programs (i.e., he/she is responsible for the operation of the data processing center and the management of the system analysts, programmers, etc.). The data processing (DP) branch may actually develop parts of the AIS or may provide technical support to the Project Manager and Sponsor/User during the system's life cycle.

Dependent upon the particular system/application under development, the ADP Manager might serve with the Sponsor/User on a system review/approval board.

2.4.2.7 Quality Assurance (QA) Specialist - The operations level QA staff is responsible for assuring the Sponsor/User that an application system is developed in accordance with the system's stated objectives, contains the needed internal controls and security to produce consistently reliable results, and operates in conformance with requirements and data processing procedures. Quality assurance, as defined in the AIS life cycle matrix, is the function that establishes the responsibilities and methods used to ensure quality in data processing products. The Quality Assurance Specialist may or may not be personally involved in establishing these responsibilities and methods.

The QA charter should allow for independent reviews. QA staff should actively participate in reviewing the development of new systems or applications and the significant modification of existing systems. (Coordination with security/audit and VV&T participants is essential to avoid duplication of effort.) In addition, the QA staff should ensure data integrity of systems. The presence and effective functioning of the QA staff will determine the nature and extent of audit involvement, in that they commonly perform similar functions.

2.5 USE OF EXTERNAL DEVELOPMENT SERVICES

2.5.1 Contractor Services

Differences in the SLC which result from the use of contractor services in lieu of in-house staff, are described briefly below. At least two points are key:

1. The term "contractor" applies to both private sector enterprises and activities of the Federal government. This latter category includes, for example, General Services Administration, Defense and non-Defense laboratories, and the National Bureau of Standards.

2. Contractors can be used in every phase and activity in the SLC. There are, however, restrictions on the type of work which contractors should do (e.g., policy formulation and management of government employees), and ways in which they should not be employed (e.g., personal services). These restrictions are stated in the Code of Federal Regulations (CFR).

Regardless of whether these services are performed in-house or contracted out, the operating environment and project management must make adequate provision for control over the system development process (e.g., requiring compliance with standards and subjecting deliverables to VV&T). Only items at variance with functions and activities specified in the AIS Life Cycle Matrix are identified, and are described in the life cycle phase in which they would occur. Differences in the audit approach, however, occasioned by the change in development circumstances, are presented following Phase VI.

2.5.1.1 Differences from the AIS Life Cycle Matrix

1. Operating Environment

- Information Resources Management (IRM) Official- Establishes guidelines on the use of contractor services, e.g., issuing design specifications for competitive award rather than automatically letting the same contractor design and develop a particular software application.

- Contracting Officer - Establishes guidelines, rules and procedures for the use of contractor services.

2. Initiation - Phase I

- Sponsor/User - In coordination with the Project Manager, incorporates a preliminary assessment of the need for contractor services in the Feasibility Study, Risk Analysis, and Cost/Benefit Analysis, where possible and as appropriate. (Minimally, the acquisition of contractor services can require a long lead time. Therefore, the impact on the project schedule must be recognized and identified.)

- Project Manager/Contracting Officer's Technical Representative (COTR) - Supports the Sponsor/User in project initiation and the assessment of government personnel and contractor resource needs.

  (No other change is required. The typical use of the contractor is in support of the Project Manager/COTR. However, contractors can also be used, for

example, by the ADP Manager to provide consultation, by the Sponsor/User to develop the Needs Statement, or by the Auditor to review/evaluate the Feasibility Study. In all cases, the government's interests must be protected by a rigorous definition of what the contractor is expected to do. It is the Contracting Officer's responsibility to ensure that the interests of the government are met. Contracting for ADP resources is discussed in GSA's 41 CFR 201-32, and is referenced in 41 CFR 210-20.003, Requirements Analysis.)

3. Definition - Phase II

   - Project Manager/COTR - Incorporates the provision of contractor resources, as appropriate, into the Project Plan to ensure that: (1) resource acquisition schedules are meaningful; (2) the role of the contractor(s) is identified and proper; and (3) objectivity controls are provided.

     (No other particular change is required. Contractors may participate in any activity unless otherwise precluded by Federal statute or Departmental policy.)

4. System Design - Phase III

   - Information Resources Management (IRM) Official- Oversees project to ensure objectivity of design with respect to requirements.

5. Programming & Training, Evaluation & Acceptance, and Installation & Operation - Phases IV, V, and VI

   No particular change is required. Contractors may participate in any activity unless otherwise precluded by Federal statute or Departmental policy.

2.5.1.2 Differences in Audit Approach - The impact on audit of using contractor services at key points in the SDLC, will vary with the degree of responsibility assigned to the contractor, and number of contractors involved. For example, at one extreme, contracts may be awarded which incorporate all major phases of the project, from feasibility study through installation and operation, into a single contract. At the other extreme, contracts may be incorporated into the project which call for limited responsibility, such as development of a single subsystem, or system documentation, or Training/User Manuals.

Care should be taken that the objective integrity of the approach is not compromised by allowing a contractor, without proper management, to define the requirements and design a

system responsive to the requirements. Without this management, there is no incentive for a contractor to seek cost-effective design approaches.

Each of the possible permutations of contractor involvement has unique characteristics which will require modification of the audit approach to specifically address the situation. There are, however, common areas which will need to be considered. The degree of audit effort directed to these areas is, of course, dependent on the nature and scope of the contractor involvement. The areas to be considered are:

- Project Plan - The overall Project Plan should include specific delineation of contractor responsibilities vis-a-vis the other "responsible participants." Particular attention should be paid to the validation, verification, testing, and certification of contractor produced products.

- Requirements Specifications - The requirements description should be as complete as possible, identifying the tasks to be completed and deliverable items, in as much detail as necessary to ensure that all documentation and decision points reflected in the AIS Life Cycle Matrix are adequately addressed, and that all relevant system development standards and guidelines are incorporated.

- Contract Monitoring - Procedures and practices relating to the monitoring and evaluation of work under the contract should be sufficient to ensure compliance by the contractor with the SDLC documentation and decision level requirements.

The audit approach to systems development activities involving contractor support remains focused on the requirements specified in the AIS Life Cycle Matrix. The use of contractors in the development process, however, does introduce additional elements for consideration in developing the overall Audit Plan. For example, the contractor should not be substituted for user involvement, project management, standards, and documentation.

2.5.2 Off-The-Shelf Software/Turnkey Systems

The acquisition and installation of off-the-shelf software or turnkey systems, in lieu of customizing a major system development effort, also requires modification of the functions or roles identified in the AIS Life Cycle Matrix. The differences in the system life cycle are as follows. (It should be kept in mind that many of the changes identified are required for the procurement of contractor services as well as software.)

2.5.2.1 Differences from the AIS Life Cycle Matrix

1. Operating Environment, Initiation (Phase I), and Programming & Training (Phase IV)

No particular change is required.

2. Definition - Phase II

- Project Manager - Prepares Functional Requirements Document to serve as the basis of procurement action.

3. Design - Phase III

- Sponsor/User - Reviews proposed procurement for sufficiency.
- Project Manager - Identifies and appoints technical evaluation panel to review technical competency of bids/offers.
- ADP Manager - Reviews requirements documents and provides technical assistance to Contracting Officer relative to development of procurement action.

4. Testing - Phase V

- Sponsor/User - Reviews results of all pre-award test procedures. Concurs in any customizing and award.
- Project Manager - Oversees completion of "live test demonstration" and other pre-award test procedures. Defines/approves required customizing. (If customizing is required, that process should be done by returning to a sub-process identical, if abbreviated, to that for full systems development Phases II-IV). Approves award to selected bidder/offeror.
- ADP Manager - Provides technical assistance in evaluating "live test demonstration" and other pre-award test procedures. Also oversees installation of software at the test site.

5. Installation & Operation - Phase VI

- Sponsor/User - Identifies and initiates request for additional modifications by manufacturer.
- Project Manager - Reviews system updates and ensures revisions to documentation and manuals, and initiates required training.
- ADP Manager - Installs licensed system updates.

2.5.2.2 Differences in Audit Approach - The major differences for the auditor in reviewing the selection and installation of off-the-shelf software will be that little to no attention will be paid to the actual coding process unless substantial customizing was required. Normally, off-the-shelf software is considered reliable unless problems are found.

However, more often than not, off-the-shelf software or turnkey systems are found to need modification to be responsive to user requirements. Any such modification may impact the agency's ability to hold the vendor accountable for problems encountered or future upgrades or maintenance. Modification to such software or to its operating environment should, therefore, be a consideration for the auditor in any of the affected life cycle phases, particularly with regard to VV&T implications.

2.6 AIS LIFE CYCLE DOCUMENTATION

Audits of systems under development are not practical unless well-defined documentation exists. System documentation requirements are a classic problem associated with the development of any automated system. The many audit reports of the General Accounting Office (GAO) support this assertion. The individual findings of PCIE Work Group members tend to corroborate the problem and the identified need. Much care was taken in the development of the documentation set presented here.

Managers may find it appropriate to either consolidate several requirements into a single document, move documentation requirements to an earlier phase, or make other changes which they deem necessary for the efficient and effective management of their program. What is critical is that the purpose and functions of the documents elaborated on below are achieved.

The purpose and general content of each of the named documents or document types identified in the AIS matrix are defined in the following paragraphs.[11] Figure 2, System Life

---

11 The references after each document type contain the requirements or justification for that document. (Note:NBS FIPS PUBS apply equally to software and the full AIS).

Cycle (SLC) Documentation Flowchart, describes the flow of documents as an AIS project proceeds through its SLC. It uses a single letter for identification of each document.

2.6.1 Needs Statement (FIPS PUB 64, DOD 7920.1, FIRMR 201-30.007)

A Needs Statement should be prepared to describe, in written form, deficiencies in existing capabilities, new or changed program requirements, or opportunities for increased economy and efficiency. It should justify the exploration of alternative solutions (including automation) to the deficiencies. An adaptation of the document should be used for systems not designated as major systems. The need for AIS security should be identified, based on anticipated system's sensitivity/criticality. Since the Needs Statement is a management document, it normally should not exceed four to six pages in length.

2.6.2 Feasibility Study (FIPS PUB 64, FIRMR 201-30.007)

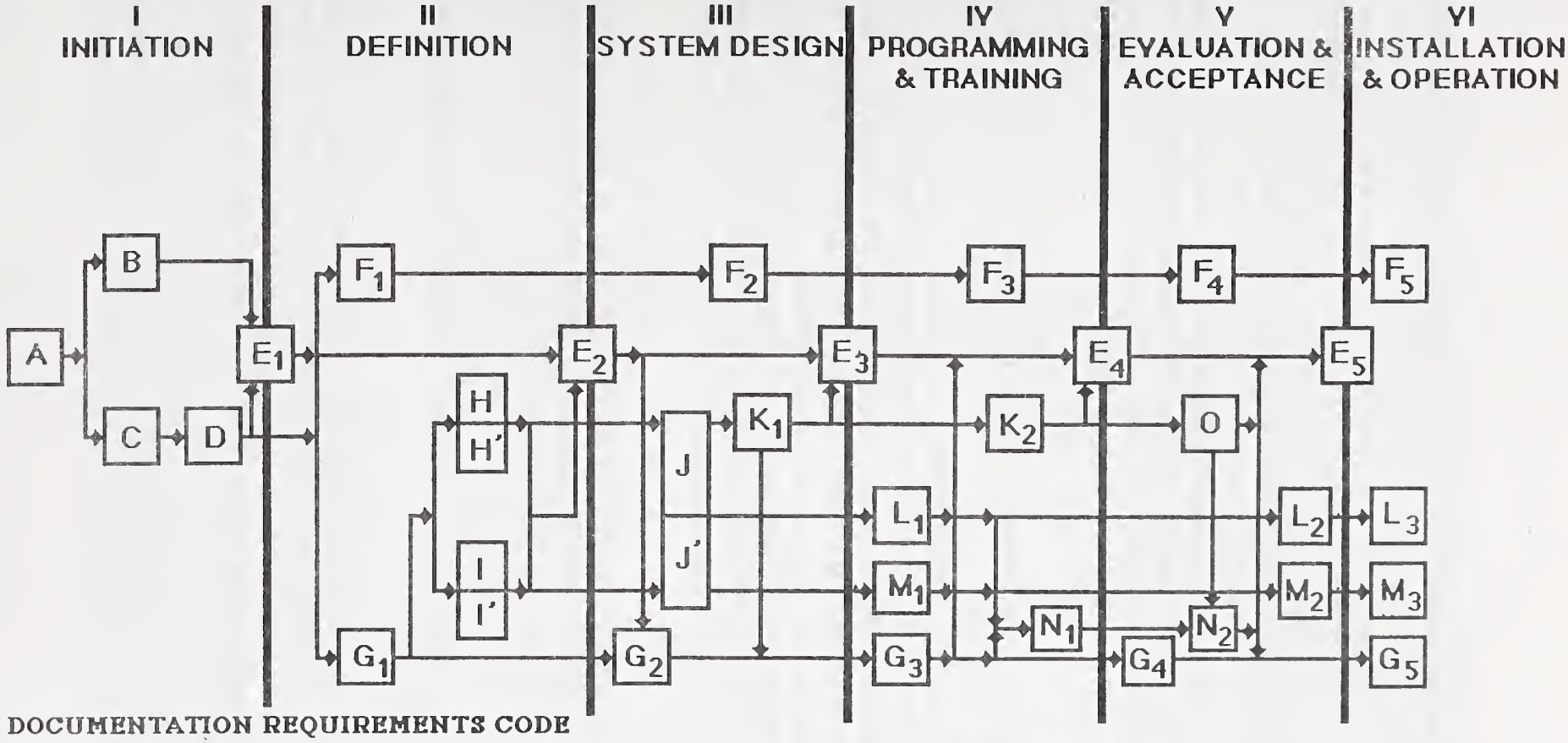
The purpose of the Feasibility Study is to provide: (1) an analysis of the objectives, requirements and system concepts; (2) an evaluation of alternative approaches for reasonably achieving the objectives; and (3) identification of a proposed approach. This study, in conjunction with the Cost/Benefit Analysis should provide management with adequate information to make decisions to initiate or continue the development, procurement, or modification of software or other ADP-related services. The Feasibility Study may be supplemented with an appendix containing details of a Cost/Benefit Analysis, or may be considered with a separate Cost/Benefit Analysis.

2.6.3 Risk Analysis (FIPS PUBS 65, 87, and 102, OMB A-130)

The purposes of the Risk Analysis are to identify internal control and security vulnerabilities of an AIS, determine the nature and magnitude of associated threats to data and assets, determine the resulting potential for loss, and provide managers, designers, systems security specialists and auditors with recommended safeguards. These would be included during the Design, Development and Installation/Operation Phases of a new and/or modified AIS to reduce the potential loss.

It should be reviewed and revised, as necessary, during each phase of the SDLC to assure that appropriate security measures are installed. The findings and recommendations of the Risk Analysis should be used by the review teams during the AIS security and certification reviews. It should be prepared and maintained as a separate document, and should be reviewed and updated as necessary, when a modification is made to the operational system.

Figure 2. SYSTEM LIFE-CYCLE DOCUMENTATION FLOW CHART



DOCUMENTATION REQUIREMENTS CODE

A. Needs Statement (FIPS PUB 64, DOD 7920.2)*
B. Feasibility Study (FIPS PUB 64)*
C. Risk Analysis (FIPS PUB 65)*
D. Cost/Benefit Analysis (FIPS PUB 64)*
E. System Decision Paper (FIPS PUB 64, DOD 7920.2)*
F. Audit Plan
G. Project Plan (FIPS PUB 102 & 105, NBS SP 500-98)*
H. Functional Requirements Document (FIPS PUB 38 & 124)*
H.' Functional Security and Internal Control Requirements Document (FIPS PUB 73 & 102)*

I. Data Requirements Document (FIPS PUB 38)*
I.' Data Sensitivity/Criticallity Description (FIPS PUB 65 & 102)*
J. System/Sub System, Program & Data Base Specifications (FIPS PUB 38)*
J.' Security and Internal Control Related Specifications (FIPS PUB 73 & 102)*
K. Validation, Verification and Testing Plan and Specifications (FIPS PUB 101)*
L. User Manual (FIPS PUB 38, NBS SP 500-98)*
M. Operations/Maintenance Manual (FIPS PUB 38, FIPS PUB 106, NBS SP 500-98)*
N. Installation & Conversion Plan (FIPS PUB 101, NBS SP 500-105)*
O. Test Analysis & Security Evaluation Report (FIPS PUB 38 & 102, NBS SP 500-98)*

* Source

(Note: Document subscripts refer to successive iterations of that document.)

2.6.4 Cost/Benefit Analysis (FIPS PUB 64, OMB A-130, OMB A-123, FIRMR 201-30.007)

The purpose of the Cost/Benefit Analysis is to provide managers, users, designers, systems security specialists, and auditors with adequate cost and benefit information, including the impact of security, privacy, and internal control requirements on that information, to analyze and evaluate alternative approaches to meeting mission deficiencies. This document, in conjunction with the Feasibility Study, should provide the information for management to make decisions to initiate or continue the development, procurement, or modification of software or other AIS-related components. The Cost/Benefit Analysis may be prepared as a separate document, or details of the Cost/Benefit Analysis may be appended to the Feasibility Study.

2.6.5 System Decision Paper (FIPS PUB 64, DOD 7920.2, OMB A-130, OMB A-123)

The System Decision Paper provides the information and framework critical to the departmental and operating divisions' decision-making process during the development of an AIS. It is the principal document for recording the essential information on the AIS, such as mission need, milestones, thresholds, issues and risks (including security, privacy and internal controls), alternatives, cost/benefits, management plan, supporting rationale for decisions, affordability in terms of projected budget and out-year funding, and the decisions made by the agency's Office of the Secretary. The System Decision Paper remains in existence throughout the life of a major AIS. It must be approved at the appropriate level when milestones for each life cycle phase are achieved.

The final iteration of the System Decision Paper, prior to the system's installation and operation, should include an accreditation statement by the responsible accrediting official, that the AIS is operating effectively. Any caveats on its operation need to be mentioned at this time.

2.6.6 Audit Plan (Public Laws Establishing OIGs, GAO Audit Standards, OMB A-130, OMB A-123, OMB A-73)

Audit Plans are developed encompassing all agency system activities. Systems under development may be selected for review based on several factors, including the sensitivity or criticality of the system or the effectiveness of internal agency ADP management control (e.g., a verification and validation group, a formalized testing process, a quality assurance function, or a risk management function).

For those systems selected for audit review, a detailed AIS specific audit plan is prepared. The plan clarifies audit involvement, which may range from audit review of completed work

products at each development stage to active review participation in each system development phase. In any case, the overall objective is to assess the adequacy of internal ADP controls and provide the "reasonable assurances" to management spelled out in Appendix 1 of the GAO Audit Standards [GAO81-1].

2.6.7 Project Plan (FIPS PUBS 102 & 105, NBS SP 500-98, OMB A-130, OMB A-123)

The Project Plan specifies the strategy for managing the software/AIS development. It defines the goals and activities for all phases and sub-phases. It includes resource estimates over the duration of system development and intermediate milestones including management and technical reviews (i.e., those for security, privacy, and internal controls requirements). In addition, it defines methods for design, documentation, problem reporting, and change control. It also specifies supporting techniques and tools.

While the focus or emphasis of the Project Plan is on the developmental phases of an AIS, the plan cannot omit consideration of the system's installation and operation, most particularly the certification process the system must go through prior to entering the final life cycle phase. A formal Certification Plan should be included as a routine subsection of the Project Plans for all systems designated as "sensitive." That subsection contains clarification of responsibilities, security requirements and evaluation approach, evaluation schedule and support required, as well as identification of the evaluation products. Just as the remainder of the Project Plan is to be reviewed and modified during each phase, so the Certification Plan is to be revised as needed, commonly based on the updated Risk Analysis.

2.6.8 Requirements Documents

2.6.8.1 Functional Requirements Document (FIPS PUBS 38, 64, 87, & 124, DOD-STD-7935, OMB A-130, OMB A-123, GSA 41, CFR 201-20) - The purpose of the Functional Requirements Document is to provide a basis for the mutual understanding between users and designers of the initial definition of the software/AIS, including the requirements, operating environment, and development plan.

It should include, in the overview, the proposed methods and procedures, a summary of improvements, a summary of impacts, security, privacy, and internal control considerations, cost considerations and alternatives. The requirements section should state the functions required of the software in quantitative and qualitative terms, and how these functions will satisfy the performance objectives. It should also specify the performance requirements vis-a-vis accuracy, validation, timing, and flexibility. Inputs/outputs need to be explained, as well as data characteristics. Finally, the Requirements Document needs to describe the Operating Environment and provide or make reference to a development plan.

2.6.8.2 Functional Security and Internal Control Requirements Document (FIPS PUBS 38, 64, 73, 87, & 102, DOD-STD-7935, OMB A-130, OMB A-123) - The purpose of the Security and Internal Control Requirements Document is to focus attention of the user and system designer on the security/internal control needs of the system, based both on vulnerabilities identified during the Risk Analysis and established internal control/security standards (e.g., GAO guidance, NBS guidance).

Included should be requirements for general controls (i.e., management and environmental controls) at the computer installation, if additional ones are needed, and automated application controls. All security requirements need to be defined and approved prior to acquiring or starting formal development of the applications.

2.6.8.3 Data Requirements Document (FIPS PUB 38, DOD-STD-7935, OMB A-130, OMB A-123) - The purpose of the Data Requirements Document is to provide, during the definition stage of software development, data descriptions and technical information about data collection requirements. The data descriptions need to be separated into two categories--static and dynamic data. Data elements in each category should be arranged in logical groupings, such as functions, subjects, or other groupings which are most relevant to their use. The document should also describe the type of information required to document the characteristics of each data element, and specify information to be collected by the user and that to be collected by the developer. Finally, procedures for data collection, and the impacts of the data requirements need to be discussed.

2.6.8.4 Data Sensitivity/Criticality Description (FIPS PUBS 65 and 102) - In the Data Sensitivity/Criticality Description, specific types of sensitive data and assets should be identified. Once sensitive/critical data have been identified, it may be necessary to determine the degree and nature of sensitivity within the general grouping. Categories of sensitivity and criticality will be agency dependent. The importance of this determination is that data sensitivity/criticality assessments need to be known before the nature and magnitude of threats can be postulated.

2.6.9 Specifications Documents

2.6.9.1 System/Subsystem, Program and Data Base Specifications (FIPS PUBS 38, DOD-STD-7935, OMB A-123, OMB A-130)[12]- The purpose of the System/Subsystem Specifications is to describe for analysts and programmers the requirements, operating environment, design characteristics, and program specifications (if desired) for a system or subsystem. The purpose of the Program Specifications is to describe for programmers, the requirements, operating environment, and design characteristics of a computer program. Both the Sys-

12 Note: These specifications are usually found in three separate documents.

tem/Subsystem and Program Specifications should have sections describing functions and performance requirements, in terms of accuracy, validation, timing and flexibility, and the operating environment. The purpose of the Data Base Specifications is to describe the nature, logical, and physical characteristics of a particular data base. The section on physical characteristics needs to address storage and design considerations.

2.6.9.2 Security and Internal Control Related Specifications (FIPS PUB 73 & 102, OMB A-123, OMB A-130) - By separating security and internal control specifications from the broader specifications papers, added weight is given to their importance. The details may be included as a separate, but clearly identifiable subsection of the other specification papers. Its purpose is to set forth security and internal control specifications to meet the functional security and internal control requirements detailed in Section 2.6.8.2.

All specifications should be sufficiently precise to allow tests to be designed which will tell whether the requirement is satisfied. The security specifications should be kept current throughout the entire life cycle of the AIS. No changes to the system should be permitted unless they either do not affect the security specifications or have been approved and entered as an official modification to the document. Security specifications should be reviewed by all organizations involved in the use or operation of the application. For any sensitive application, they must be reviewed and approved by the party responsible for security and by the organization's auditors.

2.6.10 Validation, Verification and Testing Plan and Specifications (FIPS PUBS 38 and 101, NBS SP 500-98, OMB A-130, A-123, DOD-STD-7935)

The purpose of the VV&T Plan[13] is to plan for the evaluation of quality and correctness of software, including requirements and design documentation. The VV&T Plan also provides plans for the testing of software, including detailed specifications, descriptions, and procedures for all tests, as well as test data reduction and evaluation criteria. A VV&T plan is a document, or group of documents, specifying a project's VV&T requirements and the procedures needed to achieve them. Because the general system planning drives the VV&T planning, in turn providing feedback to the overall development, the general project planning and VV&T planning are closely integrated. Once the overall background, goals, and requirements of the AIS are clearly understood, VV&T planning may begin.

---

13 Note: The VV&T Plan and Specifications may be two separate documents.

2.6.11 User Manual (FIPS PUB 38, DOD-STD-7935, OMB Circular A-130, OMB A-123)

The purpose of the User Manual is to sufficiently describe the functions performed by the software in non-ADP terminology, such that the user organization can determine its applicability, as well as when and how to use it. It should serve as a reference document for initiation procedures, preparation of input data and parameters, and for interpretation of results. In addition to general information, the manual should provide a full description of the application as well as a section on procedures and requirements, including those related to security, privacy and internal controls. It should also describe error, recovery, and file query procedures and requirements.

2.6.12 Operations/Maintenance Manual (FIPS PUBS 38 & 106, DOD-STD-7935,OMB A-130, OMB A-123)

Two separate manuals may be necessary. The purpose of the Operations Manual is to provide computer operations personnel with a description of the software and the operational environment so that the software can be run. It includes an overview of the software organization, program inventory and file inventory, as well as a description of the runs and sections on non-routine procedures, remote operations, and security requirements.

The purpose of the Maintenance Manual is to provide the maintenance programmer with the information and source code necessary to understand the programs, their operating environment, and their maintenance procedures and security requirements.

2.6.13 Installation and Conversion Plan ("Implementation Procedures (IP)" DOD-STD 7935, OMB A-130, NBS SP 500-105)

The Installation and Conversion Plan is a tool for directing the installation or implementation of an AIS at locations other than the test site, after testing of the AIS, including security features,has been completed. It may also be used to direct the implementation of major modifications or enhancements of an AIS which have already been installed. Those parts of the document directed toward users should be presented in suitably non-technical language. Those parts directed toward computer operations personnel should be presented in suitably technical terminology.

2.6.14 Test Analysis and Security Evaluation Report (FIPS PUBS 38 & 102, NBS SP 500-98, DOD-STD-7935 "Test Analysis Report," OMB A-130, OMB A-123)

The purpose of the Test Analysis Report is to: (1) document the test analysis results and findings; (2) present the demonstrated capabilities and deficiencies, including the security

evaluation report needed for certification of the AIS; and (3) provide a basis for preparing a statement of AIS/software readiness for implementation. Since it presents the deficiencies for review by staff and management personnel (i.e., users), the document should be prepared in non-technical language.

The Security Evaluation Report, which should be a large subsection of the document, should end with a certification transmittal letter and contain a suggested accreditation statement for the responsible Accrediting Official. That statement would authorize installation of the AIS, possibly with qualifications or exceptions. Agencies should conduct periodic reviews of sensitive applications, once they are operational, and recertify the adequacy of security safeguards.

2.7 DOCUMENT PHASING AND INTERRELATIONSHIPS

Figure 2 depicts the time-phasing of the documents identified and summarized in Section 2.6. Two factors are particularly worthy of note. First, each life cycle phase requires the development of certain documentation. In general, the documents are representative of the activities carried out during that phase, and are usually a prerequisite for moving to the next phase. Second, the set of documentation demonstrates multiple interrelationships. That is, they feed into other documents and/or require updating as the project moves from one life cycle phase to another.

It should also be noted that Section 2.6 and Figure 2 do not depict all of the documentation needed to assure a project's success. Workbooks, memoranda, letters, electronic mail notes, telephone logs, etc. are all part of the documentation set required for successful project communication and control. The documentation set presented here should be viewed as deliverable products resulting from the activities within a particular life cycle phase.

The following discussion should enable the auditor to better interpret Figure 2, when using it in the audit programs for the various phases.

2.7.1 Need for Flexibility

Flexibility in the interpretation of the Life Cycle Matrix is both desirable and in some instances necessary. That is, some changes to the life cycle discussed in this chapter would be appropriate if the subject to be addressed is a major modification to a system rather than the development of a new one. Similarly, modification of documentation needs might be appropriate if the system is small and uncomplicated rather than large and complex. However, the discipline and attributes inherent in the life cycle phases, participants, and documents need to be considered throughout any system development effort. Two examples illustrate this.

1. For small systems, project managers may not need a separate Validation, Verification, and Testing Plan, and may find it convenient to integrate the activity into the Project Plan, particularly during the early phases of a system's life cycle. However, the need to continually assess the user's needs (validation) and to ensure the conceptual integrity of the design (verification) are not arguable.

2. Project managers may find it efficient to integrate the results of a Feasibility Study, Cost/Benefit Analysis, and Risk Analysis into a System Decision Paper. However, the need to address the feasibility of a project, its risks, and its costs and benefits, is essential, even if the system is required by law.

2.7.2 Notation Conventions in Figure 2

The letter/number conventions and other notations used in Figure 2 reflect the following:

1. Subscripts indicate updates of a particular document based upon new information either within a particular phase, or when moving from one phase to another. Updates may not always be required, e.g., the User Manual developed in Phase IV (Programming and Training), may remain unchanged into Phase VI (Installation and Operation). This is, however, an unlikely situation for large systems.

2. The Project Plan should be updated at the beginning of each phase to serve as a coordinating medium throughout the phase. Experience indicates that the Project Plan and the other documentation as well, are often updated several times during a phase for large projects where, for example, the System Design Phase is 12 to 18 months in duration.

3. Selected documentation usually feeds into others. For example, System/Subsystem Specifications (Section 2.6.9.1) are a necessary input to the development of both the Validation, Verification and Testing (VV&T) Plan and VV&T Specifications (Section 2.6.10). Other relationships exist beyond those identified in Figure 2. These relationships should be clearly defined by the Project Manager when the program for documentation management is undertaken.

CHAPTER 3
A WORK PRIORITY SCHEME FOR THE ADP AUDITOR

3.1 INTRODUCTION

3.1.1 The Work Priority Scheme in Perspective

In Spring 1985, the PCIE Work Group (see Appendix A) co-sponsored, with ICST/NBS, a public/private sector workshop of ADP auditors, senior ADP managers, and computer security specialists who explored the criteria for assessing risk in computerized systems. (See Appendix I for participant list.) Recognizing the common problem of limitations on audit resources, the participants and their respective organizations donated two and one half days of their time to determine the most productive way to assign those resources. An NBS Internal Report No. 86-3386, released August 1986, presented the results of that workshop.

That report and this Chapter describe a high level risk analysis for AISs that can be used by computer security reviewers and ADP auditors to prioritize their non-discretionary and discretionary review activities for AISs. It divides the risk analysis problem into five areas of risk concern (called dimensions) with each area defined by a set of characteristics. Also presented are two possible risk scoring schemes, one simple and intuitive, the other method more detailed. Finally, an approach for deriving an ADP audit plan, using these scores is provided. ADP auditors are urged to use existing Risk Analyses where possible, to reduce the audit burden. The identification and risk rating of sensitive systems by ADP auditors and security reviewers should take place at the very earliest point possible so that the control requirements are identified and provided for early in the SDLC.

3.1.2 Brief Overview of the Scheme

The Scheme described in this Chapter enables its user to systematically perform a risk-based evaluation of the subjects for ADP audit (or security review) within an organization (i.e., the universe of its AISs), and to arrive at a risk measurement for each AIS. This final risk measure (or score) is based on an analysis of risk in key areas of concern (dimensions for describng risk) in that system. These scores enable the user to rank the systems by determining which AISs offer the highest levels of risk to the organization and which dimensions within each AIS contribute most to this high level of risk. Based on this analysis, the user can then draw up an ADP audit or security review work plan for the organization in question. The work plan would include annual coverage along with a basis for formulating the scope of specific AIS reviews. Considering the generality of the dimensions and their associated characteristics, the scheme is equally appropriate for public and private sector internal audit organizations.

The scheme employs a two-level review and the characteristics associated with the five dimensions. The levels and their dimensions are:

Level I
- Criticality/Mission Impact

Level II
- Size/Scale/Complexity
- Environment/Stability
- Reliability/Integrity
- Technology Integration

Each dimension is defined by a related set of characteristics which are used to estimate or calculate the amount of risk posed by that dimension to the failure of the system. A Level I review looks at Criticality/Mission Impact of the system to the organization (see Section 3.4.5.1 for Level I characteristics)and develops a risk score for each AIS with respect to this dimension. Since this dimension is the most important of the five risk areas, it can be used as a first estimate of the system risk score. The AISs can then be placed in sequence from high to low risk and the low risk systems eliminated from further review consideration. Organizations with very limited resources could stop at a Level I review and plan their work based on these results. It should be noted that some of this information may be available from already existing Risk Analyses and vulnerability assessments within the organization, and should be used so as to lower costs.

To refine the risk scores further, the high criticality risk AISs are reviewed at Level II. Risk scores are obtained for the four remaining dimensions for each high criticality risk AIS. These four dimension risk scores are summed and added to the Level I risk score to yield the system risk score for that AIS. The AISs reviewed at Level II can then again be placed in sequence from high to low risk and thus enable the reviewer or audit unit to prioritize the work.

3.2 THE NEED FOR THE SCHEME

3.2.1 ADP Audits/Security Reviews - A Form of Control

In the past ten years there has been a slowly growing recognition of the need for controls in the Federal Government's automated systems. Although there often is resistance among program sponsors or user management to employing internal controls within AISs because of the cost, time, and overhead that such controls can introduce, the interest in and use of controls in AISs is continuing to grow. This growth is augmented by the increasing emphasis OMB has placed on internal controls since the passage of PL97-255, the Federal Managers' Financial Integrity Act of 1982 [FMFIA82], and the completion and revision of their own Circular

A-123. The General Accounting Office (GAO), at Congressional request, has closely followed the Federal agencies' implementation of A-123, and, thus far, has been dissatisfied with agencies' compliance--especially in the area of internal controls in AISs.

Audit organizations, whose activities existed well before the computer age, have long recognized and stressed the need for internal controls in manual (primarily financial) systems and the need for independent audits as a critical component of the oversight of an organization's systems. With the advent of computerized AISs, career fields specializing in ADP audit (generally found in audit organizations) and security review (often found in data processing departments or management) have developed. Recognition and revision of their role in the review of automated systems is increasing rapidly.

3.2.2 Size of Review Task

A major implication of the enormous numbers of computers/systems and our dependence on them, is that the universe of AISs that needs reviewing is also enormous. The number of trained ADP auditors and security reviewers to do this job, however, has not kept pace with that growing universe. A consistent methodology for obtaining a risk score for an AIS is seen as a major tool for culling through the review work that needs to be done and assigning relevant as well as realistic workloads to the review staff available within an organization.

3.3 BACKGROUND ON THE METHODOLOGY

3.3.1 The Invitational Workshop

The PCIE Work Group, in the course of its activities, decided that an essential component of their final product, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach (this document), was a methodology for prioritizing the ADP auditor's work. Rather than rely exclusively on the experience and background of the Work Group members, it was decided to hold an invitational workshop on the subject and use the ideas generated during the course of the workshop to develop a work priority scheme.

3.3.2 Workshop Points of Agreement

Although each group came up with a somewhat different set of major audit/security concerns (dimensions) for the scheme, there was universal agreement on four underlying premises:

1. The entire ADP Audit Plan[14] must first give consideration to non-discretionary audits (mandated by law, regulation, and/or the agency/organization management). These are reflected in the front-end qualifiers (see Section 3.4.3 for list). Only if there are remaining resources for ADP audit would the scheme be used as originally intended.

2. The risk-based prioritizing evaluation needs to be performed at two levels, Level I and Level II (if sufficient resources are available).

3. The first level of inquiry (for its Level I dimension) should concern itself with the criticality of the AIS to the agency/organization mission. Only critical systems should be reviewed further (for its Level II dimensions) and given a more detailed risk score.

4. The ranking and rating of the risk characteristics of each dimension is program and agency/organization specific. Only the risk scoring method is applicable across the board.

3.4 A WORK PRIORITY SCHEME FOR THE ADP AUDITOR

3.4.1 Assumptions and Caveats

The use of the proposed work prioritizing scheme is based on certain ideal assumptions and caveats. These include:

- An inventory of all computer systems (AISs)--operational, under development, or undergoing major change--is maintained by the organization, to establish the audit universe.

- The above inventory may not be complete due to user development or system changes made outside the system development process.

- To use the priority scheme, certain minimal information is required or the assessment of the system may not be valid.

- The full priority scheme would most easily be performed by ADP audit groups in order to enlist multiple perspectives, especially where resources are known to be a concern.

---

14 It should be understood that the terms ADP audit and security review may be used interchangeably throughout the scheme.

- Auditors in the organization must agree that risk can be evaluated by a standardized scheme.

- Users should always be consulted in the risk evaluation conducted by the auditor to ensure appropriate assumptions and to assure maximum effectiveness.

- Auditor judgement is still needed!

Within this framework of assumptions and caveats the entire ADP audit work plan can then be developed. To the degree these assumptions differ from the reality of the organization's SDLC environment, the work planning methodology should be adjusted.

3.4.2 Audit Planning/Prioritization Process

The risk evaluation performed as part of the work priority scheme must be done within the context of the entire audit planning process. There are elements of the process that need to be considered prior to the risk evaluation (such as non-discretionary audit requirements), and other elements that require consideration afterwards (such as resource constraints). The following sections contain a suggested model for the entire prioritization process.

3.4.3 Non-Discretionary Audits

As can be seen from the model in Figure 3, the audit planning and prioritization process starts with front-end qualifiers that must be considered by the auditor prior to making decisions with respect to which system(s) should be audited. These front-end qualifiers consist of non-discretionary factors which are beyond the auditor's control. These nondiscretionary factors include, but are not limited to the following:

- External directives (e.g., laws, regulations, OMB circulars, and audit standards);

- Internal directives and priorities (e.g., contractual requirements; requirements, standards, and policies of audit and data processing organizations; upper management directives);

- Business/organizational environment unique to the organization (e.g., effect of economy on organization, budget of organization, and technology available to or used by organization);

- Organizational unique factors (e.g., presence and strength of quality assurance and security functions, management and control philosophy, structure, and policies);

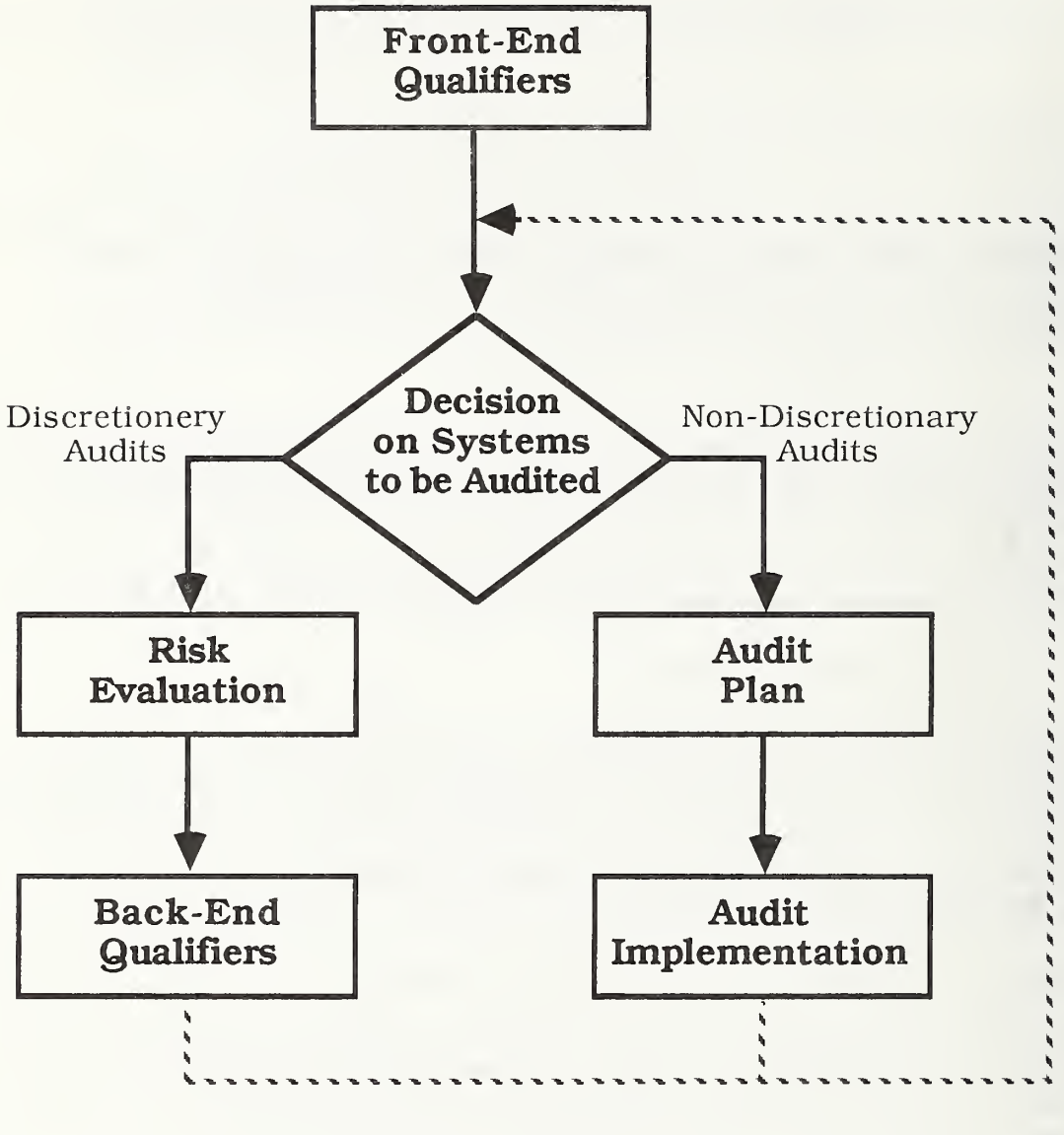


Figure 3. Audit Planning-Prioritization Process

- Geo-political environment (e.g., public concern and politics);
- Resource constraints/economic health (e.g., dollars, time, expertise, training, tools, and techniques);
- Known problems with the system, from current logs or previous evaluations and audits (e.g., nature and magnitude of problems);
- Evaluations and audits planned by management; and
- Auditor's institutional knowledge of organization's universe of systems.

After all of the front-end qualifiers have been considered, it may be that the entire audit plan is dictated by the non-discretionary work. That is, external directives, internal directives, business environment, unique organization/responsibilities, and/or resource constraints may require that certain audits be performed and these required audits may use up the limited audit resources available. In this case, the priority scheme may still be useful for determining audit approaches and where and when to focus efforts.

If, on the other hand, additional audit resources are available for discretionary audits, the risk evaluation of the work priority scheme can be used to identify and rank the systems in greatest need of audit coverage. Ultimately, back-end qualifiers may need to be considered for the discretionary audits, as described in Section 3.5.

3.4.4 Risk Evaluation Levels and Dimensions

As stated on pages 45 and 46, the work priority scheme expresses the risk concerns in terms of two levels and five dimensions. The risk concerns in Level I are reviewed first and those in Level II are reviewed second. Level I has one dimension and Level II has four dimensions. Each dimension is defined as a related set of characteristics which can estimate or measure the amount of risk posed by that dimension to a failure of the system. The chief concern of each dimension can be stated in the form of a question as follows:

1. What is the Impact/Criticality of the system to the organization?

A poorly developed or controlled system that is mission critical could jeopardize an organization's basic operational or programmatic effectiveness; therefore, an impact/critical system commands audit attention. The larger the impact, the more important it is to audit.

2. How Complex is the system? (This includes size considerations.)

The more complex the system, the more difficult is communication and control, and consequently, the higher the risk of failure. The greater the chance for failure, the more important it is to audit the system.

3. How Stable is the system internally (structure) and externally (environment)?

The less stable the system, the more difficult it is to develop procedures for communication and control, the greater the chance for failure, and the greater the need to audit.

4. How Reliable is the system and the information it processes and generates (i.e., what is the chance of the system failing or the data being wrong)?

The answer to this question is obtained by looking at the controls in the system (integrity controls) and prior audit experience. The less reliable, the more chance for failure and the need to audit.

5. How well is the Technology Integrated into the organization?

The poorer the system technology is integrated with the skills of the staff and the standards and procedures of the organization, the more chance for failure and the greater the need to audit.

These questions serve as the basis for the five dimensions itemized on page 46, and their associated characteristics developed for the work prioritization scheme.

3.4.5 Two Level Work Priority Dimensions/Characteristics

The two level work priority scheme permits a high amount of flexibility since it can be applied in any degree of detail required. For example, the results of Level I ranking may be adequate to prioritize all audit work, based on available time and resources. If additional ranking characteristics are necessary, the more detailed Level II can be used to further prioritize audit work. A two level review, additionally, enables the auditor to purge from consideration those systems which will definitely not be reviewed for any number of reasons. Environment and resource issues enter in here.

The two level work priority scheme follows in outline form, identifying the five dimensions and their related characteristics. [Note: The same characteristic may be used in more than one dimension. The question asked in each will, however, be different.]

3.4.5.1 Level I:

3.4.5.1.1 Mission Impact/Strategic Value/Organization (Business) Criticality and Sensitivity Factors

- criticality of system to organization mission
- criticality/sensitivity of system to well being, safety or interest of general public/clients-/consumers
- criticality/sensitivity of data and information
  - -competitive advantage
  - -confidence of public in program/department
  - -privacy/confidentiality/security issues
- materiality of resources controlled by system
- fraud potential
- life cycle costs of system (people and dollars)
  - -development cost budget
    - people
    - dollars
      - hardware
      - software
      - facilities
  - -operating cost budget
    - people
      - data processing/systems (including training)
      - users (including training)
    - dollars
      - hardware (CPU, peripherals, terminals, telecommunications, etc.)
        - -acquisition
        - -operation
      - software
        - -acquisition
        - -maintenance
      - supplies
      - facilities
      - configuration change control

- degree of dependence on AIS

- criticality of interfaces with other systems and external organizations

A Level I review, outlined above, provides a "first cut" at the total audit universe. This initial review will identify critical systems that require audit coverage. The additional dimensions to be reviewed in Level II should be used to rank these critical systems to find those most deserving of discretionary audit coverage.

3.4.5.2 Level II:

3.4.5.2.1 System[15] Size/Scale/Complexity

- size of user area impacted

- number/complexity of interfaces/relationships with other projects or systems

- complexity of AIS technology (e.g., network size, communication needs, system configuration, degree of centralization, nature of transaction coupling mechanisms, nature of security)

- size/complexity of system
  - -size of system budget
    - development costs
    - maintenance/operation costs
  - -number/complexity of different inputs
  - -number/complexity of unique files
  - -number/complexity of unique outputs
  - -number/complexity of logical files (views) system will access
  - -number/complexity of major types of on-line inquiry
  - -number of source documents maintained/retained
  - -number/complexity of computer programs
  - -complexity of programming language
  - -complexity of system configuration
  - -number of human elements interfacing the system
  - -number of decision levels
  - -number of functions by devices
  - -number, types, and complexity of transactions
  - -number of external organizations impacted

15 The term "system" is used in place of "project" to signify the entire AIS life cycle and the possibility of auditing at any point in the development process or operations.

- nature of interactions with external organizations

3.4.5.2.2 System Environment/Stability

- organizational breadth (interfaces, dependencies, system configuration)
- management involvement/commitment
- project management approach and structure
  -configuration management program
  -management efficiency and effectiveness
- specificity of, agreement on, and support for user requirements
- confidence in estimates--both cost and time--premising make-or-buy decisions, vendor selection, system testing/validation, etc.
- number of vendors/contractors involved
- newness of function/process to user
- problems associated with current system performance and/or system development effort
- existence/scope of data processing standards, policies and procedures, especially systems development life cycle methodology and documentation requirements
- availability of evidence - document and report preparation and maintenance for entire systems life cycle (e.g., test/validation/certification results, operations manual, system specifications, audit trails, exception reporting)
- quality and completeness of documentation
- general controls
  -physical access controls
  -environmental controls
  -communication controls
  -management controls environment
  -document controls
  -system change and test/validation/certification controls

- on-going concern issues/organization effect (will mission objectives be met in a timely manner?)
  - -interruption tolerance
  - -ability to maintain performance
  - -unsatisfactory system performance (adverse consequences from degradation or failure)
  - -unsatisfactory system development completion
  - -unsatisfactory conversion
- labor relations (e.g., salary parity, hours, fringe benefits, etc.)
- project team (management and staff effectiveness and training)
- organizational and personnel changes (frequency, magnitude, and number)
- functional requirements changes (frequency, number, and magnitude)
- technical changes (e.g., frequency, magnitude, and number)
- factors affecting cost/economic/budget climate
- availability and adequacy of back-up and recovery procedures

3.4.5.2.3 Reliability/Integrity

- hazards/risks to information system (data, hardware, communications, facilities)
- general controls
  - -environmental (e.g., physical access controls, natural hazards controls)
  - -management
- applications controls
- availability and adequacy of audit trails
- quality and quantity of automated error detection/correction procedures
- availability and adequacy of back-up and recovery procedures
- completeness, currency and accuracy of documentation for audit

- prior reviews (e.g., A-123, A-127, A-130, audits--internal, CPA, QA--IRM triennial reviews)

- auditor judgement (intuitively obvious)

3.4.5.2.4 Technology Integration

- make-up of project team in relation to technology used (number, training, and experience)

- applicability of the data processing design methodologies and standards to the technology in use

- pioneering aspects (newness of technology and/or technological approaches used in this information system for application and organization)

- technical complexity of information system (interrelationships of tasks)

- user knowledge of DP technology

- margin for error (i.e., is there reasonable time to make adjustments, corrections or perform analyses before the transaction is completed?)

- utilization of equipment (tolerance for expansion)

- availability of automated error detection/correction procedures

- completeness, currency, and accuracy of documentation for implementation-/maintenance/operation (e.g., operations/maintenance manuals).

- amount of hardcopy evidence

3.5 RISK SCORING -- APPLICATION OF THE WORK PRIORITY SCHEME

3.5.1 Implementation of the Scheme

For the scheme to be of use to the ADP auditor, an analysis approach for risk scoring must be employed using the dimensions and characteristics. Two possible approaches for arriving at a system risk score are suggested here and described in Appendix J. The first scoring method is a simple intuitive approach based on a minimal collection of information on the AIS, while the second one is more elaborate and based on more detailed information on the

AIS. User experience will undoubtedly lead to modifications and improvements in the application of the scheme and the risk scoring methods. If the ADP reviewer for some reason does not wish to use a scoring methodology, he/she could still keep the dimensions and their characteristics in mind when performing a less formal review.

3.5.2 A Simple Scoring Approach

The simple approach assigns a weight and a risk level to each dimension, based on a qualitative judgement with respect to the characteristics associated with each dimension. Criticality/ Mission Impact is always assigned the highest weight. The product of the weight and risk level of a dimension is the risk score for that dimension. The Criticality/Mission Impact risk score is then the Level I system risk score. To obtain the Level II system risk score, the sum of the dimension risk scores over the four Level II dimensions is added to the Level I system risk score. (See Appendix J for details.)

3.5.3 A Detailed Scoring Approach

The more detailed approach looks in depth at the characteristics associated with each dimension. Each dimension is defined by a set of characteristics which are used to calculate the amount of risk posed by that dimension to the failure of the system. Each characteristic is given a weight and a risk level. The product of these two numbers is the risk score of the characteristic, and the sum over the risk scores of the characteristics of a dimension yields the dimension risk score. Again, the Criticality/Mission Impact risk score is the Level I system risk score. Similarly, to obtain the Level II system risk score, the sum of the dimension risk scores over the four Level II dimensions is added to the Level I system risk score. (See Appendix J for details.)

3.5.4 Discretionary Audits

After the systems have been identified and ranked, using the risk based evaluation, several back-end qualifiers must be considered by the auditor in determining how many discretionary audits can be added to the audit plan (See Figure 3). These back-end qualifiers can be categorized in two areas:

- Audit Types and Objectives
- Audit Resource Constraints

Figure 4 identifies the different audit methodologies that can be used and the different audit objectives that can be accomplished in performing ADP audits. The auditor must consider the audit methodology to be performed and the audit objective to be accomplished in deciding on

Figure 4. AUDIT AREAS OF CONCERN*

	OBJECTIVES				
TYPES	Data Reliability	Security Confidentiality Privacy	Availability of Information Resources	Efficiency Economy Effectiveness	Compliance
(A) System Development Life Cycle Process (B) System Under Development (C) Operational Systems (Post Implementation) (D) Function, e.g., Management, Teleprocessing, Data Processing					

* Decisions on audit types and objectives desired will influence:
- Weights given when ranking risk factors
- Audit scope, i.e. level of involvement (e.g. tasks, dollars, hours)

the number of additional (i.e., discretionary) audits that can be perfomed. Furthermore, these issues must be considered in light of the audit resource constraints (e.g., people, time, dollars, expertise) that exist. For example, to perform a system under development audit which looks at security, confidentiality, and privacy issues requires substantially more resources than an operational system audit which looks at only data reliability issues. Thus, the mix of audit methodologies to be performed, and the existing audit resource constraints must be considered when deciding on the number of discretionary audits that can be added to the audit plan. After these back-end qualifiers have been considered, the audit plan can then be finalized, and audits conducted.

3.6 USES OF THE WORK PRIORITY SCHEME

The risk scores developed during the risk-based evaluation can be used for both developmental and operational systems. The major difference between risk-based evaluations of these two classes of systems is that (1) the ranking of characteristics may change, and (2) some characteristics may not be applicable to both. The following is a brief enumeration of some possible uses of the Work Priority Scheme.

1) To determine relative risk between applications - A risk score of one application is compared to scores developed for other applications in the same department. Thus, risk scoring is used to determine relative risk among applications. The score is not used to determine an absolute measure of risk.

2) To create an audit risk profile - An audit risk profile is a pictorial representation of the various risk characteristics measured. While the audit risk score shows audit risk for the entire AIS,the risk profile shows the relational risk among the various risk characteristics. The objective of the risk profile is to graphically illustrate what characteristics contribute to the total risk, and in what proportion.

3) To modify the characteristics contributing to audit risk - Both the auditor and data processing management can use the audit risk scheme to identify those characteristics which may cause the information system to be less successful than proposed. For example, if the application project personnel do not understand the computer technology being used, the probability of success of the information system being developed diminishes. Once the characteristics that may cause the system to be less successful than desired are known, those characteristics can be altered such that the probability of system success increases.

4) To help allocate audit resources - The information gathered during the audit risk analysis can be used as a basis for allocating audit resources to review application systems and/or review specific aspects of those systems. For example, high-risk information systems may receive extensive reviews, medium-risk cursory reviews, and low-risk no reviews. For

those systems reviewed, the area of review can be selected based on the high-risk characteristics. For example, if computer technology is a high-risk characteristic, the auditors may want to expend time reviewing how effectively the project team is using that technology.

5) To develop a data base of risk characteristics - The information gathered during this process should be saved and used for two purposes. The first use is to improve the audit risk prioritization scheme to make it more predictive of audit risk; the second use is to assist data processing management in structuring and planning projects such that those projects will have the highest probability of success.

3.7 PROBLEMS WITH AND SOLUTIONS TO USE OF SCHEME

Potential difficulties in using the work priority scheme and methods for overcoming these difficulties were discussed by the PCIE Work Group participants in order to facilitate the use of the scheme. These follow in outline form.

3.7.1 Potential Difficulties in Utilization

- Time and resources are needed for sufficient data collection.
- Organization data processing planning is often inadequate.
- There is a need to establish an understanding of and agreement on related issues on a consistent basis by all affected parties (auditors/systems developers/users/etc.).
- There is a need to convince affected management (audit and operations) as to the credibility of the scheme and its impact on audit coverage, given a finite level of audit resources.
- Initial time and resources are needed to adapt the work priority scheme to the organization.
- The ranking represents a snapshot at a given point in time which requires maintenance and updating to ensure its continued validity.
- Audit planning needs to be separate from and sensitive to data processing and business cycle planning processes.
- Integrated skill knowledge is required that includes relevant expertise in pertinent speciality areas.

- Work priority scheme is just another tool for audit management to consider in its decision-making process.

- ADP audit resources are still likely to be insufficient to provide coverage suggested by the scheme.

- An up-to-date and complete inventory of AISs is required--all those which are operational, developmental, and undergoing change.

3.7.2 Methods for Overcoming Difficulties

- Make the underlying questionnaire and data gathering methods as simple as possible for administering it.

- Refine data collection methods through experience and learning curve.

- Educate users (including DP community) regarding needs for standards, planning, etc..

- Audit recommendations should emphasize necessary improvements to DP and business executives.

- Encourage early participation and collective editing to reach consensus on data collection instrument.

- Apply scheme retroactively to existing systems to demonstrate the risks that audit coverage would have addressed.

- Emphasize that initial commitment would have long-term benefits and that, once established, maintenance would be considerably less costly.

- Analyze dynamics of the organization and the audit component within it to determine the frequency of the "snapshot". Workload mix and control attributes may be affected accordingly.

- Develop a means for staying atuned to planning cycles.

- Consider supplementing ADP audit resources with financial and generalist auditors for areas not requiring specific technical expertise. They may even be more relevant for business and institutional knowledge.

- ADP audit resources may be supplemented with consultants for areas requiring highly skilled data processing knowledge.

3.8 NEXT STEPS

Recognizing both the significant benefits and limitations that accompany the work prioritization scheme discussed above, what then should the ADP auditor expect to do next?

3.8.1 The Audit Organization

The NBS/PCIE workshop attendees came up with a number of recommendations for further activity by ADP Audit/Computer Security Organizations. A brief enumeration of these follows.

1) The work priority scheme described here should be tested within organizations by applying it to the ADP planning considerations of a prior year's workload universe. This might help ascertain how ADP audit resources may have been allocated differently and whether that allocation may have better assisted management in identifying and overcoming resultant control deficiencies in the systems.

2) Feedback should be captured on institutional knowledge of why and how systems have failed so that one could determine whether the draft scheme would have targeted ADP audit resources on the most vulnerable systems.

3) A prototype needs to be developed which would include a survey questionnaire, a weighting and scoring system, a testing process, a methodology for evaluating results and modifying the prototype, a method for the selection of testing sites, and a method of quantifying qualitative issues that would facilitate a comprehensive cost-benefit evaluation of the work priority scheme.

3.8.2 The ADP Auditor

Hopefully, the ADP auditor will have the opportunity to prioritize his or her work before jumping in. Whether or not the formal scheme and ranking methodology is used, however, consideration of the dimensions and their associated characteristics is strongly recommended. That review will, at the least, enable the auditor to place emphasis on those areas most vulnerable and in need of attention.

The next chapter provides detailed audit programs for each phase of the system development life cycle (SDLC) described in Chapter 2. Depending on the results of the prioritization process, the auditor might choose to emphasize one phase over another or select aspects of

each phase. The programs presented are for large critical systems that will undoubtedly require a comprehensive review. The programs can be adapted and shortened, however, for smaller sensitive systems.

CHAPTER 4
AIS DEVELOPMENTAL AUDITS

4.1 SDLC CONTROL OBJECTIVES AND AUDIT CONCERNS

4.1.1 Control Objectives

Computer data processing should produce accurate, complete, and authorized information which is supportable and timely. In a computerized environment, this is accomplished by a combination of controls in the computer application, and controls in the environment in which the computer application operates.

Controls are divided into general and application controls. General controls can be further divided into management and environmental controls. Management controls deal with organizations, policies, procedures, and planning. Environmental controls are the operational controls primarily administered through the computer center/computer operations group.

As computerized systems become more sophisticated, there is a general shift from application controls to general controls. This shift is due to the fact that some of the control functions performed by the application are shifted to the ADP environment. For example, the edit and validation data procedures may move from the application to the environment when data base concepts are used. Although the adequacy of controls over the computerized environment is growing in importance, the organization still cannot ignore the application controls area because there will always be important application controls.

This audit guide concentrates on application controls. These controls need to be reviewed for each application, while general controls should be reviewed initially but not on every application. However, even general controls require periodic review as technology, personnel, or policies change. The GAO "Black Book" [GAO81-3] provides a control assessment for evaluating general and application controls in an operational computer-based environment. This audit guide specifically addresses the process of designing application controls into a new or modified system and evaluating the entire development process.

To assist in this control evaluation, the control objectives can be divided into six categories.[16] These categories are:

1. Legal Requirements
2. Management Policies
3. Internal Controls
4. Audit Trails

16 These control objectives come from the GAO "Yellow Book" [GAO81-1]. Section 4.1.2 is taken almost verbatim from that document.

5. Documentation
6. Economy and Efficiency

4.1.2 Auditors' Control Concerns

The following material discusses the above six control objectives and the auditor concerns that they generate.

4.1.2.1 Legal Requirements - To provide reasonable assurance that systems/applications conform with legal requirements.

Legal requirements applicable to systems and applications may originate from various sources. One such requirement is compliance with State and Federal privacy statutes, which restrict collection and use of certain types of information about individuals. Safeguards are obviously necessary in such systems. Conversely, organizations subject to the Freedom of Information Act should have systems/applications designed so that appropriate and timely responses can be made to legitimate requests. The applicability of the Federal Information Processing Standards program [required by the Brooks Act [BRA65]] to the system involved should also be considered by the auditor. If such standards apply, they should be included in the auditor's review.

Once again, auditor review of the design and development processes can help assure management that these requirements have been considered and satisfied.

4.1.2.2 Management Policies - To provide reasonable assurance that systems/applications carry out the policies management has prescribed for them.

Policies on what is expected of automated systems should be established by management, and the auditor should determine whether they are being adhered to in design. The auditor should ascertain whether an appropriate approval process is being followed, both in developing new systems and in modifying existing systems. The auditor should consider the need for approval of a system's design by data processing management, user groups, or other groups whose data and reports may be affected. Also, the auditor should review the provisions for security required by management, to protect data and programs against unauthorized access and modification.

If management's requirements are not being met, or have not been clearly articulated, the auditor must report such shortcomings to officials who can take corrective action. Frequently, in the past, efforts to make new systems/applications operational by scheduled dates have resulted in some elements or controls that were desired by management being set aside by designers for later consideration. Auditors, in retaining their independence during the design and development processes, should report such actions to top management for resolution.

4.1.2.3 Internal Controls - To provide reasonable assurance to management that systems/applications include the controls necessary to protect against loss or serious error.

The system design and development processes include: (1) defining the processing to be done by a computer; (2) designing the processing steps; (3) determining the data input and files that will be required; and (4) specifying each individual program's input data and output. Each area must be properly controlled, consistent with good management practices. The auditor's review of these matters is designed to provide reasonable assurance to management that the systems/applications, once placed in operation, will be protected against loss or serious error.

Properly designed systems, with excellent control mechanisms built in, might have these controls bypassed or overridden by management direction. This has occurred in systems immediately after they were implemented and put into operation. Many times the designers and developers override such controls to get the system operational and then forget to activate the controls after the system errors have been corrected.

Almost every system has manual aspects (e.g., input origination, output disposition), and these, together with the electronic data processing controls, are considered when the auditor is reviewing system controls for adequacy.

4.1.2.4 Audit Trails - To provide reasonable assurance that systems/applications provide the controls and audit trails needed for management, auditor, and operational review.

In financial applications, a transaction must be capable of being traced from its initiation, through all the intermediate processing steps, to the resulting financial statements. Similarly, information in the financial statements must be traceable to its origin. Such capability is referred to by various terms (e.g., audit trail, management trail, transaction trail) and is also essential in non-financial systems or applications. The reliability of the output can be properly assessed when the transaction processing flow can be traced and the controls over it, both manual and automated, can be evaluated.

During the design and development process, the auditor may recommend, through formal correspondence, audit trails or other controls to the design/development team. By doing so through formal correspondence, the auditor will remain independent.

Audit of the systems design and development processes can help assure management that this capability is in fact being built into the systems/applications.

4.1.2.5 Documentation - To provide reasonable assurance that systems/applications are documented in a manner that will provide the understanding of the system required for appropriate maintenance and auditing.

The auditor should determine whether the design, development, and modification procedures produce documentation sufficient to define: (1) the processing that must be done by programs in the system; (2) the data files to be processed: (3) the reports to be prepared: (4) the instructions to be used by computer operators; and (5) the instructions to user groups for preparation and control of data. The auditor should also ascertain whether management policy provides for evaluation of documentation and adequate testing of the system before it is made operational. These steps are taken to ensure that the system and its controls can be relied on.

4.1.2.6 Economy and Efficiency - To provide reasonable assurance that systems/applications will be efficient and economical in operation.

Determining whether an organization is managing and using its resources (e.g., personnel, property, space) efficiently and economically, and reporting on the causes of inefficiencies or uneconomical practices, including inadequacies in management information systems, administrative procedures, or organizational structures, is considered here as a basic characteristic of government program audits. With the development of complex systems or applications, the auditor's review should also focus on whether the system has been developed in such a way that operations will produce desired results at minimum cost. For example, early in a system's development, the auditor should review the adequacy of the: (1) statement of mission needs and system objectives; (2) Feasibility Study and evaluation of alternative designs to meet those needs and objectives; and (3) Cost/Benefit Analysis which attributes specific benefits and costs to system alternatives.

4.2 APPROACH FOR SYSTEMS UNDER DEVELOPMENT

4.2.1 Introduction

The mid-level ADP auditor is presumed to fully understand the basic SDLC process and to have a basic familiarity with the specific SDLC process utilized within the organization under review. With this familiarity the ADP auditor only needs to survey the organization's current SDLC process to ensure a complete and accurate understanding of the currently existent procedures and responsibilities. The survey should be structured around the AIS Life Cycle Matrix (see Chapter 2) and may involve a "preliminary review of the SDLC methodology" (see Section 4.2.2). Additionally, an audit survey for each SDLC phase is incorporated in Sections 4.3 through 4.7 for consideration in developing the scope of review throughout the SDLC process. The survey scope is impacted by the effectiveness of the organization's quality assurance function as well as its utilization of appropriate technologies, and its methodologies for software development and system installation. These impacts on the survey scope are further discussed in Section 4.2.3.

The rest of this chapter is designed primarily to assist the mid-level ADP auditor in designing and conducting audits of the development of AISs that are in process. The chapter

is divided into the SDLC phases as reflected in the AIS Life Cycle Matrix described in Chapter 2. It prescribes audit coverage for consideration throughout the AIS development cycle. The audit approach and considerations for each phase, however, are presented as separate modules for use in review during the AIS developmental phase, or at the completion of a particular phase.

Each module within the rest of this chapter is presented in a parallel manner for a consistent and comprehensive description of potential audit coverage for each AIS developmental phase. The modules each contain the following segments:

1. Audit participation - Brief introduction of the phase and relevant audit involvement.
2. Primary audit objectives - Overall purpose for audit coverage during phase.
3. Overview - Description of the phase and its AIS life cycle matrix responsibilities and deliverables.
4. Audit survey - Initial background analysis and pertinent survey technique(s).
5. Customized audit objectives - AIS phase developments impacting scope of subsequent audit coverage.
6. Detailed audit testing - Specific audit objectives, tests, and techniques.
7. Assessment of audit results - Analyses for developing and reporting phase audit test results and planning future AIS audit coverage.
8. Questionnaires/Matrices - Tools for soliciting and assimilating pertinent phase information.

4.2.2 Preliminary Review of the SDLC Methodology[17]

The SDLC methodology described in this audit guide is a conceptual methodology. It incorporates good practices from many different methodologies into one approach. From an audit perspective, it defines the type of documentation needed to ensure the auditability of an AIS.

Auditors involved in system development reviews should not expect to find the system developed precisely according to the methodology described in this audit guide. The auditors should expect that the methodology used by the organization encompasses the best parts/documents of the methodology described herein. If the development methodology is deficient, the auditor should recommend improvements in that methodology along the lines of that defined in this audit guide.

---

17 This section is based on work done by the Internal Audit Steering Committee organized and chaired by Coopers and Lybrand, New York. The material found here has been incorporated in the IIA published document "System Development Audit Review Guide" [C&L86] that resulted from this committee's efforts.

The auditor has two tasks to perform in reviewing the SDLC methodology being used to develop the system the auditor is reviewing. First, the auditor must make a preliminary review of the system development methodology (SDM) for its adequacy in providing the discipline and control over the AIS development as prescribed in this guide. Second, the auditor must compare the SDLC being used for the AIS under review with this guide's methodology, for coverage of its provisions and the adequacy of the control over the AIS development.

4.2.2.1 Review the SDLC Methodology to be Used in Developing the AIS Under Review - The following represents an audit program to review the organization-specific SDM. This program should be used for the following two purposes:

1. Prior to performing any development review, the auditor should become familiar with the organization's SDM. The objective is to familiarize the auditor with the processes that will be followed and documents produced, as the system is being developed.

2. Prior to each development phase review, the auditor should review the methodology applicable to that phase. This review will help reconcile the SDM used for the AIS under review, with the review program and documents described in this audit guide. The steps that the auditor needs to take to perform a preliminary review of a SDM either the entire methodology or the methodology for a single phase of the development cycle, are:

   1) Obtain a copy of the SDM used by the organization to develop and monitor the development of new applications or systems. By interviewing agency personnel, determine whether requirements are mandatory or advisory in nature.

   2) Determine whether any prior evaluations have been performed on the methodology and review them for background information.

   3) Through observation, interview, and review of available evidence determine whether:

      (a) The methodology as documented is up to date, and applications or systems are being developed in compliance with it.

      (b) There are any known problems with the methodology as it exists.

      (c) Deviations from the formal methodology are permitted.

4) By reviewing documentation and interviewing key agency personnel, evaluate the effectiveness of the SDM as follows:

(a) Is it formally structured into phases, each yielding a measurable end product?

(b) Do identifiable closure points exist for each designated phase that require the completion of formalized documentation?

5) Is emphasis placed on the incorporation of security and internal controls (including audit and quality assurance tools and techniques) into systems being developed, ensuring that they are consistent with management objectives?

6) Are planning requirements for each subsequent phase clearly identified?

7) Does the methodology allow for controlling changes in requirements over the life of the project?

8) Has an ADP steering committee been established to review the system development process, assign priorities to projects, and resolve problems as they arise? Does it include senior departmental officials?

9) Does the SDM formally recognize participation of the following groups or personnel in the development process:

(a) Sponsor/User,
(b) Project Manager,
(c) Data Processing,
(d) Quality Assurance,
(e) System Security/Internal Control, and
(f) Audit?

10) Have responsibilities for the participant groups in (9) above been formally established for each designated phase?

11) Are the roles and responsibilities of the members of the data processing project team or its equivalent clearly defined (e.g., system analyst, system designer, programmer, data analyst, data base administrator)?

12) To ensure that the needs of users and the organization are met at each phase, does the methodology provide sufficient opportunities for communication between users and system developers?

13) Do well-defined written standards exist to facilitate adequate documentation?

14) Are the requirements for user, program, system and operations documentation for each phase adequate and clearly identified?

15) Do well-defined written standards exist for programming?

16) Has the methodology incorporated considerations for:

(a) database environments,
(b) telecommunications,
(c) networking,
(d) distributed processing,
(e) end user programming (fourth generation),
(f) prototyping, and
(g) packaged software selection and implementation?

17) Are Project Managers authorized to make decisions on personnel, resources, scheduling, costs, budgets, and most technical project matters?

18) Are Project Managers sufficiently supported by top management to accomplish the system development project?

4.2.2.2 Compare Organization's SDLC Methodology to Audit Guide SDLC Methodology - Once the auditor has reviewed and understood the SDLC methodology being used for the AIS under review, that methodology should be compared to the methodology described in this audit guide.

This step involves the following tasks:

1. Compare the documents described in this audit guide to the documents in the SDLC methodology used for developing the AIS under review. The documents may have a different name, or they may be consolidated into fewer documents or split apart into more documents. The task involves determining if comparable documented information is contained in both methodologies.

2. Identify deficiencies in the SDLC methodology used in developing the AIS under review. This list can include either documents, or attributes of documents which are missing from the methodology.

3. Determine the audit importance of missing documents or document attributes. The auditor needs to determine whether the lack of those documents will have any significant impact on the AIS. This determination can be made by reading Sections 4.3 to 4.7 about the use and review of the information in those documents.

4. If the missing documents or document attributes are significant, the auditor should recommend that the methodology be corrected, particularly for this AIS, to provide that missing information.

4.2.3 AIS Development Impact on Audit Scope

As reflected in Section 4.2.1, the mid-level ADP auditor's scope of audit coverage will be impacted by the organization's SDLC process as well as the characteristics of the individual AIS under development. During the preliminary review of the SDLC methodology and the specific AIS audit survey, the auditors will be identifying and assessing the various impacts on their audit scope, and correspondingly aligning the necessary resources and expertise to execute the appropriate audit coverage.

The AIS impacts on or implications for the audit's scope may relate to the effectiveness of controls within the organization's SDLC methodology or to the capabilities of the organization to effectively incorporate available technologies and SDLC disciplines. For example, an effectively controlled SDLC methodology instituted in an organization, as evidenced by previous AIS development audit coverage or through a preliminary SDLC review, may allow the auditors to confine their scope to a survey of the effective application of this methodology to the specific AIS under review. Furthermore, while the auditors are absolutely independent of those responsible for the SDLC process, the auditors' scope could also be curtailed after verifying the effectiveness of quality assurance activity during the AIS development. Unfortunately, a quality assurance function is a control within a SDLC process which has been formally instituted in only a few organizations. It is differentiated from ADP audit which independently assesses the whole SDLC process, including the quality assurance function's effectiveness.

Other SDLC methodology implications could compel the auditors to expand their planned audit coverage or to supplement their assigned audit resources with specific expertise. Where historical audit coverage has evidenced SDLC control weaknesses in a phase, expanded audit coverage may be needed. Examples of such weaknesses may include: a)

introduction of new technologies without commensurate in-house expertise; b) utilization of system testing methods without adequately protecting the security or integrity of data; c) software development through purchased off-the-shelf applications without providing for necessary interfaces or customizing; and d) procurement of system design and development without adequate evaluation criteria or expertise to effectively oversee contracted work.

These and other AIS development implications should be evaluated for their potential impact on the AIS as well as their impact on the audit scope and corresponding audit resources. The audit survey should result in audit objectives customized to reflect these implications. Their impacts should also be reflected in the detailed audit tests and again considered when assessing audit results.

Should the auditors be unable to properly complement their resources with the necessary expertise or should other constraints be placed on the audit coverage, the AIS development review report should be qualified accordingly.

4.2.4 The Effect of a Quality Assurance (QA) Function on the ADP Auditor's Role in the SDLC

The labels, definitions, and substance of QA can vary substantially among organizations. One or more of the following might apply to the organization's concept of QA: design review, independent testing, peer review, requirements review, walk-throughs, product assurance, standards compliance enforcement, code review, and data integrity review.

The QA definition for purposes of this audit guide is: Any mechanism used by management which provides assurance that a quality product (requirements, design, code, etc.) is being developed. If management has an effective QA function in one area, the ADP auditor can concentrate efforts on other more vulnerable areas. Unfortunately, the mechanism management has in place may be perfunctory and only give the illusion of quality, e.g., peer review might be a pro forma paper exercise with little analytical criticism and no corrective action. To determine the effectiveness of QA and its effect on audit activities, several steps should be taken at the start of the SDLC or during a phase.

1. Determine what QA mechanisms are in place. The question to be directed to management is "How are you assured that products have quality (i.e., other than personal assurances from systems personnel)?"

2. Evaluate QA mechanisms (i.e., what physical evidence is there that the mechanisms actually work?). The evidence can be in the form of reports to management, documentation of reviews or a prior audit of the process.

3. Modify audit plans where QA is effective (e.g., if it can be established that standards are effectively enforced, the auditor may not need to review the adequacy of documentation).

4. On the other hand, if significant problems are identified with the QA function, the auditor should recommend strengthening the function, particularly for this AIS, to provide the needed oversight function.

4.3 AUDIT PARTICIPATION DURING THE INITIATION PHASE - PHASE I

During the Initiation Phase, the need for a computerized solution to a problem is identified and validated. Alternate methods for satisfying the need are explored and a functional recommendation is developed. The recommendation is presented to management, and if approved the AIS project continues through the remaining phases of systems development.

The primary audit objective during this phase is to ensure that the system need is established and that the cost for satisfying that need is justified. The auditor will perform the review of the Initiation Phase by examining the documents produced during that phase, and interviewing the Initiation Phase participants and other involved parties. The result of the audit review of this phase becomes an input to management in determining whether or not to approve the Initiation Phase recommendation.

4.3.1 Primary Audit Objective of the Initiation Phase

The primary objective of reviewing the Initiation Phase is to:

"Ensure that the system need is established and that the cost to satisfy that need is justified."

The achievement of that audit objective will require the auditor to review the documentation produced during the Initiation Phase. The documentation is reviewed for two reasons: first, to ensure that the documentation is complete and in compliance with the organization's Initiation Phase; and second, to ensure the accuracy and completeness of the established need and the reasonableness of the cost-justification for accomplishing that need.

4.3.2 Overview of the Initiation Phase

Consistent with the FIPS PUB 64 "Project Request Document" [FIPS64] and DOD "Mission Analysis" and "Concept Development" Phases [DOD78-2], the Initiation Phase begins with the recognition of a problem and the identification of a need. During this phase, the need is validated, and the exploration of alternative functional concepts to satisfy the need is recommended and approved. The decision to pursue a solution must be based upon a clear under-

standing of the problem, a preliminary investigation of alternative solutions, and a comparison of the expected benefits versus costs (including design, construction, operation, and potential risks) of the solution. At this stage the risk/sensitivity of the data or information in the AIS should be evaluated.

During the Initiation Phase it is immaterial whether the solution will be in-house-developed software, contracted software, or off-the-shelf software. The objective of this phase is to look at alternate functional solutions to the user need. No particular change to the SDLC methodology for this phase is needed regardless of which of the three potential implementation methods are selected later in the developmental process. Likewise, the audit approach remains unchanged during this phase, whether or not the system is developed in-house or obtained through contracting or purchase.

4.3.2.1 Participants and Their Tasks - Listed below are the responsible participants in the Initiation Phase with a brief description of their role during the phase, including the role of the auditor:

1. System Security Officer(SSO)/Internal Control Officer(ICO) - Oversees or conducts Risk Analysis; helps evaluate system sensitivity.

2. Auditor - Reviews/evaluates Needs Statement, Feasibility Study, Risk Analysis, and Cost/Benefit Analysis; based upon review determines scope of future involvement.

3. Sponsor/User - Identifies and validates need; develops Needs Statement; directs Feasibility Study, Risk Analysis, and Cost/Benefit Analysis; selects a Project Manager.

   If all or part of the SDLC effort will be contracted, the Sponsor/User in coordination with the Project Manager, incorporates a preliminary assessment of the need for contractor services in the Feasibility Study, Risk Analysis, and Cost/Benefit Analysis, where possible and as appropriate. (Minimally, the acquisition of contractor services can require a long lead time; therefore, the impact on the project schedule must be recognized and identified.)

4. Project Manager/Contracting Officer's Technical Representative (COTR) - If appropriate, awards contract and assures contract compliance. The Project Manager/Contracting Officer's Technical Representative (COTR) supports the Sponsor/User in project initiation and the assessment of government personnel and contractor resource needs.

5. System Security Specialist(SSS)/Internal Control Specialist(ICS) - Provides consultations as appropriate.

6. Contracting Officer - If appropriate, awards contract.

7. Contract Auditor - If appropriate, assures contract compliance.

8. ADP Manager - Provides technical consultation as appropriate.

9. Quality Assurance (QA) Specialist - Provides consultation on quality attributes of Needs Statement.

4.3.2.2 System Initiation Phase Documents - The Initiation Phase audit will focus on the documents produced during this phase. While the actual documents produced will vary from agency to agency depending upon their system development methodology, the more common documents produced during the Initiation Phase are:

1. Needs Statement (FIPS PUB 64, DOD 7920.2, FIMR 201-30.007) - A Needs Statement should be prepared to describe in written form deficiencies in existing capabilities, new or changed program requirements, or opportunities for increased economy and efficiency. It should justify the exploration of alternative solutions.

2. Feasibility Study (FIPS PUB 64, FIRMR 201-30.007) - The purpose of the Feasibility Study is to provide: (1) an analysis of the objectives, requirements and system concepts; (2) an evaluation of alternative approaches for reasonably achieving the objectives; and (3) identification of a proposed approach.

3. Risk Analysis (FIPS PUB 65 and 102, OMB A-130) The purpose of the Risk Analysis is to identify internal control and security vulnerabilities of an AIS, determine the nature and magnitude of associated threats to data and assets, and provide managers, designers, systems security specialists and auditors with recommended safeguards to be included during the design, development, and installation/operation phases of a new or modified AIS.

4. Cost/Benefit Analysis (FIPS PUB 64, OMB A-130, OMB A-123, FIRMR 201-30.007) - The purpose of the Cost/Benefit Analysis document is to provide managers, users, designers, systems security specialists and auditors with adequate cost and benefit information, including the impact of security, privacy and internal control requirements on that information, to analyze and evaluate alternative approaches to meeting mission deficiencies.

5. System Decision Paper (FIPS PUB 64, DOD 7920.2, OMB A-130, OMB A-123) - The System Decision Paper (SDP) provides the information and framework critical to the departmental and operating divisions' decision-making process during the development of an AIS.

4.3.3 Audit Survey

In preparing for the Initiation Phase review, the auditor needs to understand the work flow, gather the necessary documentation, and interview the responsible participants. Most of this background analysis can be done within the team established to implement the project. The tasks that need to be completed during the audit survey are to: (1) study the environment in which the project will be initiated; (2) review Initiation Phase plans; (3) gather information on the Initiation Phase status; and (4) verify information on the Initiation Phase status. The four tasks are discussed individually below.

4.3.3.1 Study the Initiation Phase Environment - Prior to conducting the review of the Initiation Phase, the auditor should:

1. Become familiar with the developing organization's system development life cycle (SDLC) methodology with particular emphasis on the methodology in the Initiation Phase. Specific review tasks should include:

   (a) Determine whether any prior evaluations of this SDLC methodology have been made, and if so how its effectiveness was evaluated.

   (b) Determine if the development team understands and supports the SDLC methodology.

   (c) By inquiry and review of documentation, evaluate the effectiveness of the SDLC methodology.

   (d) Compare the SDLC methodology to that defined in this audit guide and note differences, particularly where problems might occur due to development deficiencies.

   (e) Identify the documents produced by the SDLC methodology.

   (f) Determine through interview whether the project team has been adequately trained in the use of the SDLC methodology.

2. Become familiar with the organization's cost-justification process.

3. Become familiar with the appropriate regulations/policies relating to the area being considered for automation.

4.3.3.2 Review Initiation Phase Plans - The auditor should become familiar with the problem that has been recognized and the need to be satisfied. The plan to initiate the AIS should be reviewed to ensure that it will result in the type of documents described in this subsection. The auditor should also inquire about Initiation Phase participants to ensure that the participants identified in this subsection will in fact participate in the Initiation Phase.

4.3.3.3 Gather Information on the Initiation Phase Status - The auditor should obtain and review the following Initiation Phase documents:

1. Needs Statement
2. Feasibility Study
3. Risk Analysis
4. Cost/Benefit Analysis
5. System Decision Paper

The auditor needs to determine status information in three areas. First is the status of the above five documents, i.e, whether they have been prepared, and if so, whether in accordance with the SDLC methodology. Second is the status of the project, i.e., whether it is on time, and whether the needed tasks have been completed, and if not, when their completion is expected. Third, the auditor should identify any changes in the identified problem or need, and validate that those changes have been properly incorporated into the documents developed during this phase.

4.3.3.4 Verify Information on Initiation Phase Status - In fulfilling this task, the auditor should review the documents produced during the Initiation Phase, and interview key participants about their role in the preparation of those documents.

4.3.3.4.1 Review Documents - The Initiation Phase produces five major documents. An AIS project begins with a Needs Statement. This statement either includes, or is supported by, a needs validation and justification statement. The Sponsor/User of the system must in some manner be able to justify undertaking the AIS Initiation Phase. In previous system development audits it has been frequently noted that valid alternatives have not been considered during the Initiation Phase. Therefore, the auditor should be particularly sensitive to ensure that this has occurred for the system under review.

The Needs Statement becomes the basis for a Feasibility Study and a Risk Analysis study. The objective of these parts of the Initiation Phase is to identify a proposed approach and the vulnerabilities associated with that approach.

The Risk Analysis provides additional input to supplement the Needs Statement so that a Cost/Benefit Analysis can be prepared. This document, in conjunction with the Feasibility Study document, provides the necessary information for management to make a decision to initiate or continue the development, or to take other appropriate actions. The actions of management will be included within a System Decision Paper. This becomes the principle document containing the essential information about the AIS. It becomes a basis for the system Definition Phase.

Note that different SDLC methodologies may produce slightly different documents. In some organizations, the information defined within these five documents may be consolidated into fewer documents, or expanded into a greater number of documents. What is important from an audit perspective is that the information included in these five documents is developed during the Initiation Phase.

The documents to be completed during the Initiation Phase will be specified by the agency's SDLC methodology. The auditor, having gained a familiarity with that methodology during the background step, can determine that all of the appropriate documents have been prepared. The auditor should ensure the appropriate accumulation of information for the System Decision Paper, in order to verify the correctness of that document.

4.3.3.4.2 Interview Key Participants - The auditor should identify the responsible participants in the Initiation Phase, and interview them to determine that the needed Initiation Phase tasks have been performed. A list of the responsible participants and the questions that should be asked of those participants is provided below. The objective of this background task is to ensure that the work necessary to properly prepare a System Decision Paper has been performed. In specific organizations the participants may have different titles than those listed below, or the tasks may be divided in a different manner. It is not as important that the tasks be performed by the indicated responsible participant as it is that the tasks are performed (by someone).

1. Sponsor/User tasks
   (a) Has the Sponsor/User developed a Needs Statement?
   (b) Has the Sponsor/User identified and validated the needs?
   (c) What direction did the Sponsor/User provide for the preparation of an Alternatives Analysis, a Feasibility Study, a Risk Analysis, a Cost/Benefit Analysis, and a System Decision Paper?
   (d) Has the Sponsor/User selected a Project Manager?

2. Project Manager/Contracting Officer's Technical Representative (COTR)
   (a) Has the Project Manager/COTR developed or overseen development of an Alternatives Analysis, a Feasibility Study, a Risk Analysis, a Cost/-Benefit Analysis, and a System Decision Paper?

3. System Security Specialist/Internal Control Specialist
   (a) Has the System Security Specialist/Internal Control Specialist provided security and/or internal control consultation as appropriate?

4. Contracting Officer
   (a) Has the Contracting Officer, if appropriate, awarded the contract?

5. Contract Auditor
   (a) Has the Contract Auditor, if appropriate, assured contract compliance?

6. ADP Manager
   (a) Has the ADP Manager provided Initiation Phase consultation as appropriate?

7. Quality Assurance Specialist
   (a) Has the Quality Assurance Specialist, if the function exists, provided consultation on quality attributes of the Needs Statement?

If the needed background information and/or the needed involvement by responsible participants has not occurred,the auditor should report that potential vulnerability in the Initiation Phase audit report. The failure to perform these tasks may result in an incomplete and/or inaccurate System Decision Paper.

4.3.4 Customize Audit Objectives

Unless the Initiation Phase is conducted in accordance with the process defined in this audit guide, the auditor will need to customize the audit approach based on the agency's particular SDLC methodology. In addition, if the software is to be contracted or purchased there will be other considerations.

4.3.4.1 SDLC Methodology Audit Considerations - The Initiation Phase is designed to produce information leading to an implementation decision. In many instances, the decision to implement the system is made after the problem has been recognized and the need defined, and before any other information is collected and analyzed. In those instances, the project team may not prepare the types of documents defined in this phase program.

Rather than four distinct documents leading to a decision paper, some organizations only prepare a single document which may be called a "Needs Analysis" document. Within this document they tend to incorporate all of the components of the five major documents described for this phase. The auditor should not be particularly concerned about the number of documents prepared, but should concentrate on the information in those documents to ensure it contains the same type of information as described in the five documents in this phase. Unless that information is prepared, the full facts needed for decision and later implementation will not have been developed.

In some instances the information may not be fully documented. Some installations prepare oral presentations to initiate projects, with the documented information only on visual aids. In those instances, the auditor should attempt to sit in on the presentation, or go over the presentation with the presenters shortly thereafter.

During this phase or at its conclusion, the auditor will be reviewing the established need and the cost-justification for implementing that need. In most Initiation Phase reviews, this will involve evaluating the proposed system in the context of the agency mission. However, there may be nondiscretionary factors which could affect the extent and scope of the Initiation Phase review. The factors that would affect the extent and scope of the Initiation Phase audit include:

1. Laws, regulations, OMB circulars, and other audit standards directing audit involvement in the program being computerized.

2. Requirements included in contractual provisions or other requirements defining audit role during systems development.

3. A business or organizational environment which because of its unique factors (e.g.,the size of the budget of the organization) warrants additional audit attention.

4. Presence or absence of internal assessment groups (e.g., ADP quality assurance, or specialized staff groups, such as computer security officers) necessitating greater or lesser audit involvement.
5. Applications which are politically sensitive (e.g., environment related applications).

6. Resource constraints on the audit organization (e.g., the lack of budget, expertise, or tools to do the appropriate audit function).

7. Past history of the agency/application which indicates abnormal activity (e.g., previous GAO reports identifying agency/application vulnerabilities).

The presence or absence of these types of factors may result in changing the scope of the audit (e.g., lead to a more detailed evaluation of the need for the system, or identification of factors which could significantly change the effort/resources needed to implement the system).

4.3.4.2 Contracting/Purchase Audit Considerations - If the project may result in the acquisition and installation of off-the-shelf software, in lieu of customized software, there is no particular change required for the Initiation Phase. Changes in the developmental process would not occur until the next phase (i.e., Definition - Phase II).

There are additional considerations if there is a probability that the software will be contracted to an independent vendor. The typical use of the contractor is in support of the Project Manager/COTR. Contractors can also be used, however, by the ADP Manager, to provide consultation to the Sponsor/User to develop the Needs Statement, or by the Auditor, to review-/evaluate the Feasibility Study. In all cases, the government's interests must be protected by a rigorous definition of what the contractor is expected to do. It is the Contracting Officer's responsibility to ensure that the interests of the government are met. Contracting for ADP resources is discussed in GSA's 41 CFR 201-32, and is referenced in 41 CFR 201-20.003, Requirements Analysis.

The decision to use a contractor resides with the Sponsor or User,in consultation with the Project Manager. The analysis to determine whether or not a contractor should be used would be included in the Alternatives Analysis, Feasibility Study, Risk Analysis, and Cost/Benefit Analysis. The conclusions drawn from these aspects of the Initiation Phase will indicate the desirability of contracting out the software development.

If the use of off-the-shelf software or an independent contractor has not been included as an alternative, the auditor should investigate why these alternatives have not been considered. If a contractor alternative is included, the auditor should evaluate whether or not that alternative has been given appropriate consideration, and that the alternative selected is reasonable.

In systems that are to be completed through contract/purchase, the following concerns should be addressed by the auditor:

1. Has a COTR been assigned to the project?

2. Is it known whether this type of software can be purchased/contracted for in the public sector?

3. Are there any security considerations that might prevent this need from being satisfied through contract/purchase?

4. Are adequate funds available for contract/purchase?

5. Are there any strong business/organization reasons that might preclude the work being done by other than agency staff?

6. Is there adequate time to go through the purchasing/contracting procedure?

7. Will the system specifications be firm enough at the point of contracting/purchasing to provide the vendor with sufficient information to develop an appropriate system?

4.3.5 Detailed Audit Testing

4.3.5.1 Introduction - The auditor should select those documents and criteria within documents, that have a significant effect on the management decision to proceed with the project. Those items should be tested through additional audit investigation and tests. The recommended tests for the Initiation Phase are included in the Initiation Phase detailed testing program. (See Table 4.1)

4.3.5.2 Systems Initiation Phase Audit Tests Program - The program contained in this guide (see Table 4.1) indicates the audit objectives/indicators to be evaluated. For each audit objective/indicator, there are one or more audit tests to be performed. Where appropriate, tools and techniques are listed to assist the auditor in performing these tests. Note that in some instances the audit tool or technique consists of a general description, while in other instances the program refers to a specific product or document containing a specific audit approach for the indicated test.

4.3.5.3 Survey Questionnaire - Initiation Phase - The auditor has two verification tasks to perform. First, the auditor must ensure that the appropriate forms, worksheets, and documents have been prepared as specified by the system development methodology. Second, the auditor must verify that the information has been properly recorded on the documents. The extensiveness of these verification tests will be dependent upon the specific audit objectives selected.

In organizations having a quality assurance (QA) function, QA normally performs this verification task. In those instances, the auditor need only test to determine whether or not the quality assurance review is in place and working effectively.

The documents to be completed during the Initiation Phase will be specified by the agency's system development methodology. The auditor, having gained a familiarity with that methodology during the background step, can determine that all of the appropriate documents have been prepared. The auditor should ensure the appropriate buildup of information into the System Decision Paper in order to verify the correctness of that document.

The Needs Statement should include:

1. Expression of need in terms of agency mission;
2. Deficiencies in existing capabilities;
3. New or changed program requirements needed;
4. Opportunities for increasing economy and efficiency of user operation;
5. The internal control/security needed for the AIS; and
6. Alternative solutions to solving the need with justification for the alternatives being proposed.

The Feasibility Study should include:

1. An analysis of the objectives, requirements, and system concepts;
2. An evaluation of alternative approaches for reasonably achieving the objectives;
3. Identification of the proposed approach; and
4. Sufficient information in the above three areas, or additional areas, to provide management with adequate information to make decisions to initiate or continue the development, procurement, or modification of software or other ADP-related services.

The Risk Analysis should contain:

1. Identification of internal control and security vulnerabilities;
2. The nature and magnitude of associated threats to data and assets covered by the proposed AIS;
3. Recommended safeguards to be included in the design to address the identified risks; and
4. A detailed review of all data and assets to be processed or accessed by the system, showing the value and sensitivity of that data or assets.

The Cost/Benefit Analysis should include:

1. Costs to build the system;
2. Benefits to be derived from the system;
3. Impact of the AIS on security, privacy, and internal control requirements;
4. Analysis and evaluation of alternative approaches proposed in meeting the mission deficiencies; and
5. Detailed Cost/Benefit Analysis of the proposed alternative.

The System Decision Paper should include:

1. Information and framework critical to the decision-making process;
2. Mission need;
3. Milestones;
4. Thresholds;
5. Issues and risks;
6. Alternatives;
7. Cost/benefits;
8. Management plan supporting rationale for decisions;
9. Affordability in terms of projected budget and out-of-year funding; and
10. The decision made (alternative selected).

4.3.6 Audit Results/Reporting

Problems identified in the previous audit steps should result in audit recommendations, assuming the variance identified is significant. The auditor should be able to identify the potential impact of the variance prior to issuing an audit report recommending corrective action. The audit report should be released prior to management's decision on whether or not to proceed with the AIS (i.e., sign-off on the System Decision Paper).

4.3.6.1 Potential Deficiencies - The objective of the review is to determine whether the Initiation Phase contains deficiencies. Any such deficiencies should be reported, together with recommendations to overcome them. However, while specific deficiencies are unique to an individual AIS, experience has shown that certain deficiencies are more prevalent than others. These problems are listed below as a basis for comparison against deficiencies identified in the review. They assist the auditor in assuring that these more common deficiencies have not been overlooked.

1. The Needs Statement will not be complete, and thus the possibility that the implemented system will not meet the true needs of the user.

2. A reasonable set of alternatives will not be considered, and thus the alternative selected might not be the best alternative.

3. The right individuals from user management might not be involved, or sufficiently involved, in the Initiation Phase, resulting in a decision which may not be fully supported by user management. This is particularly true when two or more departments/agencies are involved in the same system.

4. All vulnerabilities may not be identified, or the magnitude of those vulnerabilities may not be determined, which could result in extensive additional costs or operational vulnerabilities.

5. The Cost/Benefit Analysis does not identify all of the costs, or the benefits may be overstated, resulting in a system being implemented which should not be.

6. The System Decision Paper may not include all important elements uncovered during the phase, resulting in an incorrect decision due to lack of information.

7. The System Decision Paper may not be reviewed by a sufficient number of involved managers to have that paper adequately evaluated, resulting in the implementation of a system which may be deficient or overly costly.

4.3.6.2 Potential Effects of Deficiencies on Meeting System Mission - The impact of the identified deficiencies on completing the system mission must be determined. In order for user management to make effective decisions on audit findings and recommendations, they need an assessment of the impact of those deficiencies on their mission. The auditor can use the strategies for determining the value of an impact, as described in FIPS PUB 65, or can use information readily available and collected during the Initiation Phase review.

4.3.7 Reassess Audit Strategy

The audit of the Initiation Phase should conclude with a determination of the audit strategy for the remaining developmental phases. The audit strategy should include:

1. Extent of audit involvement in the remaining system development phases.

2. Schedule of audit tasks, to be coordinated with the system development schedule.

3. Specific auditor assignments. [Note: It is advantageous to have continuity in audit staff throughout the entire developmental process unless specialists are required for a single phase audit.]

4. Audit tools and techniques to be used. [Note: Some tools require unique skills and extended preparatory time.]

The audit strategy will be affected by the auditor's analysis of the Initiation Phase work. The criteria which could extend or reduce the projected audit involvement in the remaining phases include:

1. Outside directives impacting the scope and extent of audit involvement.

2. Competency and involvement of other internal groups providing an independent assessment of the AIS (e.g., the quality assurance function).

3. The completeness and accuracy of the documents produced during the Initiation Phase.

4. The apparent consensus of involved parties regarding the correctness of the alternative selected.

5. The assurance that can be placed on the Cost/Benefit Analysis and Risk Analysis.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	User Needs Statement clearly defines the need/problem and justification for implementing that need.	1. Determine that the user organizations have been identified.	Compare organizations identified in the Needs Statement with the agency's organization chart to ensure that all appropriate users have been identified in the Needs Statement. Compare the Needs Statement to the appropriate user organization mission to ensure that the need serves the mission.
		2. Determine that the description of the need is in written form and includes the following expression of need in terms of agency mission: a) Description of current function b) Deficiencies of current function c) Resources expended on the current function d) Volumes of work produced with the current function, including peak processing performance plus projected growth e) Statutory/regulatory mandates f) Internal control/security requirements g) Justification for improvement and changes h) Scope and objectives of proposed system	Distribute user satisfaction questionnaire (included in GAO "Black Book"[GAO81-3]) to identified users to verify the existence of deficiencies/problems/ needs in the current system.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	(continued)	i) Alternative solutions to solving the need j) Interrelationships with other systems k) Relationship with long-range plans and other IRM initiatives [For additional questions, see DOL87, 2C,D,E,F on p. IV-10 and 2C,D on p. IV-29.]	
2.	User department(s) management should participate in the project Initiation Phase.	1. Review appropriate documentation to validate user participation, such as: a) Minutes of steering committee meeting for evidence of user department management participation b) Review the project plans to determine the nature and extent of user department participation c) Review user management to determine management's budgets for time allocation to efforts related to the project. 2. Interview user management to determine their understanding and level of participation in the project.	Locate appropriate documents and assess the reasonableness of user management participation. Structured interview techniques.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	The Feasibility Study docu-ment should be clearly defined and docu-mented.	1. Determine that the objectives and problem statement of the project have been described in such a manner that the objectives may serve as measure-ments of systems effectiveness during and after the system development. 2. Determine that the analysis of alternatives is well documented. a) Verify there is a list of all identified alternatives and a description of how each alternative will alleviate the problem. b) Confirm with the user that no reasonable alter-natives were omitted from the study. c) Verify that the alternatives are described in suf-ficient detail to adequately support the time and cost estimates, cost/benefit analyses, and impact studies. This is to challenge the reasons for selecting or rejecting alternatives. d) Verify that the analyses of the alternatives described in c) above apply comparable criteria in a consistent manner.	Evaluate each objective from the perspective of whether or not that objective could be used in an in-process audit during system development and in a post-implementation review to measure whether or not the system has achieved its objec-tives. Also relate the system objectives back to the Needs Statement. Ensure that the alternatives include, at a mini-mum, the information and analysis prescribed in FIPS PUB 64 and, if possible, the SDLC methodology being used.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)	e) Verify that the alternatives are technologically feasible considering the level of the technical knowledge of the organization, and the level of sophistication of the proposed alternatives. f) Verify that the alternatives meet user requirements. g) Verify that the alternatives reflect official standards. 3. Determine that a technological Feasibility Study was prepared and documented for each alternative and that the technology is feasible, considering the technical sophistication existent or available through the organization. a) Review the technological Feasibility Study report to see if it has adequately addressed: 1) Hardware needs and availability 2) System software needs and availability 3) Communications hardware and software needs and availability 4) Valid time constraints in the user department's information requirements and the manner of satisfying them 5) Operational feasibility, such as whether the new project fits into the current mix of hardware, software, and communications environment	

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)	6) Feasibility Study assumptions and constraints 7) The criteria used for the Feasibility Study b) Review the technological Feasibility Study report to see if it has considered: 1) Legal considerations related to interstate or international transfer of data 2) Regulating constraints related to the use of technology and the manner of securing regulating authority's concurrence or approval c) Verify that there is a consensus among user departments and designers concerning the technological aspects of the system's configuration. d) Determine the organizational capability to manage the related technologies and whether the technologies would potentially be developed, operated, and maintained in-house or contracted out. e) Confirm with independent sources the reliability and track record of the recommended hardware and software. 4. Determine that the recommended course of action is adequately substantiated as the most feasible.	

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)	5. Determine that, for vendor-supplied packages: a) Options/alternatives were considered. b) Specified modifications were made c) Contractual provisions were met [For additional questions, see DOL87, 2P,Q, pp. IV-30-31.]	
4.	AIS internal control and security vulnerabilities should have been determined, as well as the magnitude of associated threats.	1. Determine that a risk management team has been formed, that it included the appropriate individuals, and evaluate the reasonableness of the following risk team tasks: a) Review the list of identified vulnerabilities b) Verify that the magnitude of each vulnerability has been stated c) Verify that the vulnerabilities address all aspects of the application, including telecommunication links, contingency planning, etc. d) Verify that all known risks in existent systems are fully considered. e) Verify that recommended safeguards are included in the design to address the identified risks.	To evaluate reasonableness of the results, assess the makeup of the risk management team, the performance of that team through the documented minutes and reports, the methodology used, and the completeness of the results against the vulnerabilities and risk analysis methodology described in FIPS PUB 65, OMB Circulars A-130, A-109, and A-123.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
4.	(continued)	1. Determine that the analysis of the project costs and benefits was prepared to evaluate the economic feasibility of each alternative.	
5.	Cost/Benefit Analysis should include all of the cost and benefit considerations associated with the initiation, operation, and maintenance of the AIS.	a) Review the summary of present systems costs as well as estimated costs of each alternative to ascertain that all costs have been included in the summary. b) Evaluate assumptions and constraints in the Cost/Benefit Analysis for reasonableness. c) Verify that user and system costs cover all phases of the SDLC. d) Verify that estimated costs for an alternative include hardware and software enhancements needed to support that alternative, where applicable. e) Verify that estimated costs for an alternative include costs of security and internal controls, training, data preparation and entry, file conversion, testing, parallel operations, acceptance, and related costs, where applicable. f) Verify that the basis of estimation and computation of costs appear to be reasonable.	Compare the type and extent of cost/benefit information developed during the project to the categories of cost/benefit information included in FIPS PUB 64. Ensure that the information has been summarized in a manner consistent with that specified by FIPS PUB 64.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
5.	(continued)	f) Verify that the basis of estimation and computation of costs appear to be reasonable. g) Verify that benefits are quantified where possible. h) Verify there is a substantial consensus among end users, design developers, and implementors concerning system costs, benefits, and contractual requirements. i) Verify that the benefits claimed appear to be reasonable. [For additional questions, see DOL87, 2H-Q, pp. IV-34 to 37.]	
6.	Management should review the Feasibility Study reports and decide whether to proceed. When the decision is made to proceed, one of the alternatives should be selected as the starting point for the following system development phases.	1. Verify that the System Decision Paper has been disseminated to all user management for analysis and approval. 2. Verify that the paper is approved by the senior/responsible IRM office. 3. Verify that if the decision is made to proceed with the AIS, that the alternative selected is the one included in the System Decision Paper.	Structured interview technique. Compare the documented management decision on the AIS to the System Decision Paper to verify that the alternative selected is included in the System Decision Paper.

TABLE 4.1 - INITIATION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
7.	Validate that an analysis was made prior to programming to determine whether the work could have been done more economically through contracting and/or purchasing off-the-shelf software.	1. Review the documentation in the phase to determine that alternate means of obtaining code were given adequate consideration.	Structured interview - Meet with involved personnel to validate through documents and interview that appropriate consideration was given to alternate implementation methods. Manuals such as DATAPRO and DATA DECISIONS provide listings of software by general category. This can be used to determine if a software package is available in the application area.

4.4 AUDIT PARTICIPATION IN THE DEFINITION PHASE - PHASE II

During the Definition Phase, the functional requirements are defined, and detailed planning for the development of an operational AIS is begun. Experience has shown that it is difficult to obtain a good requirements definition. GAO studies of AISs show inadequate requirements statements to be one of the major causes of defects in AISs. Because of the difficulty in defining correct requirements the first time, requirement identification should be an iterative process.

The audit objectives during the Definition Phase are to ensure that user needs have been clearly defined and translated into requirements statements, including requirements for a system of internal control designed to conform to established standards. This audit objective will be accomplished primarily through an independent analysis of the Definition Phase documents and the validation of the information contained in those documents.

4.4.1 Primary Audit Objective of the Definition Phase

The primary audit objective for the Definition Phase is:

"To ensure that users' needs have been clearly defined and translated into requirements statements which incorporate adequate controls and conform to established standards."

In accomplishing this objective, the auditor will have to understand the needs identified during the Initiation Phase. This is necessary to ensure that the Definition Phase properly translates those needs into appropriate requirements statements. In addition, many auditors emphasize internal control requirements because experience has shown that to be a major weakness in the Definition Phase.

In order to perform this audit phase effectively, the auditor must become familiar with the Definition Phase of the agency's SDLC methodology. This will require an understanding of the Definition Phase work flow and the documents produced during that phase. The auditor will also need to identify the participants in the Definition Phase, and determine their specific responsibilities.

4.4.2 Overview of the Definition Phase

In the Definition Phase, the needs from the Initiation Phase are translated into a computer solution. The system designers must develop the logic which will permit user needs to be accomplished on a computer. This is achieved through the involvement of individuals from user and data processing areas, and involved third parties such as internal control and security personnel.

The Definition Phase will produce the functional requirements and begin detailed planning for development of an operable AIS. Functional requirements and processes to be automated are documented and approved by an appropriate senior management official before the AIS development effort is begun. Requirements identification is iterative, as is the analysis of potential risk, involving those who both identify and solve problems. It is critical that internal control and specific security requirements be identified during this process. Requirements may be modified in later phases as a better understanding of the problem is gained. Also, during the Definition Phase, a Project Plan specifying a strategy for managing AIS development, certification, and accreditation is prepared. It defines the goals and activities for all phases, and includes resource estimates during each phase and intermediate milestones, as well as methods for design, documentation, problem reporting, and change control.

The physical number of participants in this phase is normally greater than the Initiation Phase. Data processing personnel play a much more active role during the Definition Phase. Improperly defined requirements usually surface during definition.

4.4.2.1 Participants and Their Tasks - The responsible participants in the Definition Phase, together with a brief description of their responsibilities follows:

1. Information Resources Management (IRM) Official - Approves Needs Statement to advance to Phase II (Definition), in consultation with Sponsor/User and ADP Manager. (Note: This occurs between phases I & II.)

2. System Security Officer (SSO)/Internal Control Officer (ICO) - Reviews SSO/-ICO components of Project Plan, Functional Requirements Documents and Data Requirements Documents, on a selective basis.

3. Auditor(OIG) - Reviews/evaluates System Decision Paper, Project Plan, Functional Requirements Documents, Data Requirements Documents and participates in their development, as necessary; identifies audit trail and auditability requirements, including quality assurance and audit tools and techniques, for incorporation in requirements documents; prepares Audit Program.

4. Sponsor/User - Approves Project Plan and Functional and Data Requirements Documents, and updates System Decision Paper.

5. Project Manager/Contracting Officer's Technical Representative (COTR) - Develops Project Plan, Functional and Data Requirements Documents with Sponsor/User participation and audit consultation.

6. System Security Specialist/Internal Control Specialist - Provides consultation and review of SSO/ICO components of Project Plan, Functional Requirements Documents and Data Requirements Documents.

7. Contracting Officer - If appropriate, awards contract.

8. Contract Auditor - If appropriate, assures contract compliance.

9. ADP Manager - Reviews Validation, Verification and Testing components of Project Plan, Functional Requirements Documents, Data Requirements Documents, as appropriate; provides technical support to Project Manager and Sponsor/User.

10. Quality Assurance (QA) Specialist - Reviews project definition to ensure compliance with Needs Statement and data processing standards.

4.4.2.2 System Definition Phase Documents - The work performed during the Definition Phase will be recorded on six major Definition Phase documents. In addition, the System Decision Paper will be updated as appropriate. Furthermore, each phase of the system life cycle provides an opportunity to reevaluate the risks, cost/benefit, and approach to be taken during implementation. Regardless of the developmental methodology employed, the auditor can expect to find approximately the same information produced.

The six major documents produced in this phase and a brief description of their contents follow. Note that the major laws, regulations, and directives that require or recommend these documents are found in parentheses after each document name.

1. Audit Plan (Public Laws Establishing OIGs, GAO Audit Standards, OMB A-130, OMB A-123) The objective is to assess the adequacy of internal ADP controls and provide the "reasonable assurances" to management spelled out in Appendix 1 of the GAO Audit Standards (Yellow Book).

2. Project Plan (FIPS PUBS 102 & 105, NBS SP 500-98, OMB A-130, OMB A-123) The Project Plan specifies the strategy for managing the software/AIS development. It defines the goals and activities for all phases and subphases.

3. Functional Requirements Document (FIPS PUBS 38, 64, & 124, DOD-STD-7935, OMB A-130, OMB A-123) The purpose of the Functional Requirements Document is to provide a basis for the mutual understanding between users and designers of the initial definition of the AIS, including the requirements, operating environment, and development plan.

4. Functional Security and Internal Control Requirements Document (FIPS PUBS 38, 64, 73, & 102, DOD-STD-7935, OMB A-130, OMB A-123) The purpose of the Functional Security and Internal Control Requirements Document is to focus attention of the user and system designer on the security/internal control needs of the system, based both on vulnerabilities identified during the Risk Analysis and established internal control standards. This document may be included as an appendix to the Functional Requirements Document.

5. Data Requirements Document (FIPS PUB 38, DOD-STD-7935, OMB A-130, OMB A-123) The purpose of the Data Requirements Document is to provide, during the definition stage of software development, a data description and technical information about data collection requirements.

6. Data Sensitivity/Criticality Description (FIPS PUBS 65 and 102, OMB A-123 and 130) Based on an assessment of sensitivity and/or criticality, provides a general statement of the nature and magnitude of potential threats for use in the formal Risk Analysis, and preliminary determination of data sensitivity. This document may be included as an appendix to the Data Requirements Document.

In addition to the six major documents produced in this phase, one document, the System Decision Paper, is updated.

4.4.3 Audit Survey

The audit survey in this and following phases will primarily involve review of: (1) the documents produced in the previous phase; (2) appropriate audit workpapers produced in the previous phase; and (3) those documents produced in the present phase. The audit survey in the Initiation Phase required the auditors to look at the user area and appropriate policies, regulations, and the SDLC methodology. That information should be documented in the audit workpapers from the Initiation Phase.

The objective of the survey in this and the remaining phases is to bring the auditor "up to speed" in review activities. If the phases were short in duration, the survey in this and later phases may not be necessary. However, in most instances, several weeks or months may elapse between the conclusion of one phase and the point where the auditor re-enters the development process to conduct the review during the following phases.

Each survey will involve four steps. First, the auditor will need to review the output documents produced in the previous phase plus appropriate audit workpapers. Second, the auditor must review and become familiar with the plans to complete this phase. Third, the auditor gathers the documentation produced during this phase and evaluates the status of work in com-

parison to the plan. Lastly, the auditor verifies the documents produced during this phase through challenging and analyzing those documents, as well as interviewing the participants in the phase. Note that the specific work within these four tasks will be dependent upon the customized audit objectives selected for this phase (see Section 4.4.4). These four tasks are discussed individually in the following sections.

4.4.3.1 Review Initiation Phase Outputs - The auditor should review the following five Initiation Phase documents, or the equivalent documents produced by the developmental methodology used for this AIS:

1. Needs Statement
2. Feasibility Study
3. Risk Analysis
4. Cost/Benefit Analysis
5. System Decision Paper

The key document for review is the System Decision Paper. This will include a summation of much of the information in the other documents. The auditor should refer back to the other documents as appropriate to get more detailed information.

The auditor should review the audit workpapers prepared during the previous phase. The major concern here is to review the deficiencies uncovered during the Initiation Phase. The auditor, during this review, will want to ensure that those deficiencies have been adequately addressed during the Definition Phase. One of the major audit tasks in each review phase is to evaluate the adequacy of the actions taken on auditor-identified deficiencies from the previous phase.

4.4.3.2 Review Definition Phase Plans - The System Decision Paper should provide the details of the plan for implementing each phase. However, the auditor should be aware that many organizations maintain their schedules and plans through automated scheduling and project management systems. In these instances, the auditor may need the outputs from the automatic scheduling system in order to review the plans.

The key plans, from an audit perspective, are the tasks which will produce the needed documentation. Thus, the auditor should study the documents to be produced during the phase, and then relate those to the plans to ensure that they will be produced during the phase. If it is uncertain that all the needed information will be produced, the auditor should challenge the adequacy of the plans.

4.4.3.3 Gather Information on Definition Phase Status - The auditor should monitor project status periodically to determine when reviews should occur. This can be done through

questioning project management, or through querying automated project status systems. The auditor should not rely upon the project personnel to identify when a review is to occur, unless management has imposed the restriction that the phase is not complete until it has been reviewed by audit.

The auditor needs to determine the status of three aspects of the project. First is the administrative status of the project, which is a budget and schedule status. This is necessary to determine where the project stands and its availability for review. Second, the auditor needs to determine the status of documentation. [Note: The fact that the administrative schedule indicates a document is complete does not necessarily indicate that all of the attributes of that document have been completed.] If schedule and budget are tight, the project team may decide to eliminate certain parts of documents in order to stay on schedule. If this is done, the auditor should note those missing items as project deficiencies. Third, the auditor wants to determine the status of changes. If there have been significant changes to the project, the auditor will want to ensure that the schedule and budget have been adjusted accordingly, and any changes needed to the documents produced in previous phases have been made.

4.4.3.4 Verify Information on Definition Phase Status - This task involves reviewing documents produced during the Definition Phase and interviewing the key participants who produced those documents.

4.4.3.4.1 Review Documents - The construction of an AIS is performed in conjunction with development of a series of documents that build one upon another. The information used for the project's Definition Phase originates from the Initiation Phase System Decision Paper. This information is then supplemented and expanded upon through the processes which produce the Definition Phase documents.

The document flow for the Definition Phase is determined by the SDLC methodology. The System Decision Paper is the source document for both the Project Plan and the updated System Decision Paper. [It is also the source document for the Audit Plan, but that will be prepared by the audit function, as opposed to the developmental group. See Section 4.4.7 on audit strategy for the tasks needed to develop the Audit Plan.] The Project Plan specifies the strategy for managing the software development process. The Project Plan also indicates how the system will be certified prior to installation and operation.

The System Decision Paper plus the Project Plan are used as the basis for developing the Functional Requirements Document, the Functional Security and Internal Control Requirements Document, the Data Requirements Document, and the Data Sensitivity/Criticality Description. The preparation of these documents requires extensive interaction among the responsible participants. The interaction primarily involves the responsible functional/opera-

tional participants, although the policy/oversight participants will be contributing expertise in their specialty areas.

All of the documents developed during this phase, with the exclusion of the Audit Plan, are also utilized to update the System Decision Paper. The auditor wants to ensure that the System Decision Paper's currentness and completeness is maintained throughout the entire development process. It is at this point in the cycle that management again must make a decision regarding the continuation of the project. Management has the option to continue the project through the next phase, cancel the project, or propose modifications to the project. This may cause parts or all of the Initiation and Definition Phase to be repeated.

4.4.3.4.2 Interview Key Participants - The auditor has two concerns regarding the participants responsible for the Definition Phase; first, that the appropriate individuals participate, and second, that they perform the proper functions. To do this, the auditor should identify who is participating in the Definition Phase, and the roles and responsibilities of those individuals.

Listed below are the areas of recommended involvement:

1. Information Resources Management (IRM) Official
   (a) Has the IRM official approved Needs Statement prior to commencing Phase II (performed in consultation with Sponsor/User and ADP Manager)? Note that this occurs between the end of Phase I and the start of Phase II.

2. System Security Officer (SSO)/Internal Control Officer (ICO)
   (a) Has the SSO/ICO reviewed security/control components of the Project Plan?
   (b) Has the SSO/ICO reviewed security/control components of the Functional Requirements Document?
   (c) Has the SSO/ICO reviewed the security/control components of the Data Requirements Document? [Note: This may be done on a select basis as deemed necessary by the SSO and ICO.]

3. Sponsor/User
   (a) Has the Sponsor/User approved the Project Plan?
   (b) Has the Sponsor/User approved the Functional Requirements Document?
   (c) Has the Sponsor/User approved the Data Requirements Document?
   (d) Has the Sponsor/User developed/modified the System Decision Paper prior to the completion of the phase?

4. Project Manager(PM)/Contracting Officer's Technical Representative(COTR).
   (a) Has the PM/COTR developed a Project Plan?
   (b) Has the PM/COTR developed Functional Requirements Documents (with user participation)?
   (c) Has the PM/COTR developed a Data Requirements Document (with user participation)?

5. System Security Specialist(SSS)/Internal Control Specialist(ICS).
   (a) Has the SSS/ICS provided consultation and review of the SSO/ICO components of the Project Plan?
   (b) Has the SSS/ICS provided consultation and review of the SSO/ICO components of the Functional Requirements Document?
   (c) Has the SSS/ICS provided consultation and review of the SSO/ICO components of the Data Requirements Documents?

6. Contracting Officer
   (a) Has the Contracting Officer awarded the contract, if appropriate?

7. Contract Auditor
   (a) Has the Contract Auditor assured contract compliance, if appropriate?

8. ADP Manager
   (a) Has the ADP Manager reviewed the Project Plan?
   (b) Has the ADP Manager reviewed the Functional Requirements Document?
   (c) Has the ADP Manager reviewed the Data Requirements Document?
   (d) Has the ADP Manager provided technical support, as appropriate, to the Project Manager?
   (e) Has the ADP Manager provided technical support, as appropriate, to the Sponsor/User?

9. Quality Assurance (QA) Specialist
   (a) Has QA Specialist reviewed project definition to ensure compliance with Needs Statement?
   (b) Has QA Specialist reviewed project definition to ensure compliance with data processing standards?

Note that in some agencies, all of these positions will not exist; however, the tasks indicated for those responsible participants should be performed. The auditor should first ensure

that they are performed, and then ensure that the individual performing them has the necessary skills and responsibility to perform them effectively.

4.4.4 Customize Audit Objectives

The previously stated audit objectives must be modified for the specific AIS. The auditor must identify the specific user needs that must be traced to clearly defined requirements statements, and the established standards to which controls must conform. This involves the creation of a set of specific audit objectives for the Definition Phase.

The extent of audit involvement in the Definition Phase will be partially dependent upon a series of factors that can cause the AIS to have greater impact on the agency. Also, the greater the number of factors that may negatively impact the success of the AIS, the greater the need for audit involvement during this phase. That involvement should be reflected in the customization of audit objectives.

4.4.4.1 SDLC Methodology Audit Considerations - The type of documents and information produced during the Definition Phase will be heavily dependent upon the prevailing managerial style and philosophy. For example, if the managerial style is to anticipate risks, much emphasis will be placed on the Risk Analysis. Likewise, if management is very concerned about the Cost/Benefit Analysis, attention will be placed on creating that document. On the other hand, if these are areas of little interest to management, only cursory attention may be paid to these documents.

The auditor may also encounter automated SDLC methodologies. In those instances, the developers will enter the information electronically; the information may not be printed in hard-copy format. The auditor will either need to learn to use the system to review the information, or have someone print the information for audit purposes.

4.4.4.2 Contracting/Purchase Audit Considerations - There are minimal changes in the audit approach during the Definition Phase, whether the AIS is developed in-house, purchased off the shelf, or contracted for. However, two responsibilities are changed during the Definition Phase, and these will require the auditor to verify that those added responsibilities are performed during the background/survey audit step. These changes are:

1. Off-the-shelf software change -
   If off-the-shelf software is being considered, then the Project Manager, in preparing the functional requirements, must prepare that document to serve as the basis for procurement action.

2. Contracting difference -
If it is expected that the software will be acquired through contract, the Project Manager/COTR must incorporate the provision of contractor resources, as appropriate, into the Project Plan to ensure that: (1)resource acquisition schedules are meaningful; (2)the role of the contractor(s) is identified and proper; and (3)controls are provided for contractor objectivity.

No other particular changes are required. Contractors may participate in any activity unless otherwise precluded by Federal statute or departmental policy.

The specific contracting/purchase Definition Phase concerns that should be addressed by the auditor include:

1. Does the phase define the type of contractors/vendors that will be eligible to perform this project?

2. Do benefits outweigh costs through the use of purchased/contracted software?

3. Will the contractor/vendor be able to deal with the significance of identified vulnerabilities/risks?

4. Has the COTR been sufficiently involved in the definition process to determine whether adequate information has been developed to begin the contracting or purchase?

5. Have measurement criteria been established which can be used to evaluate the product produced by a contractor/vendor?

4.4.5 Detailed Audit Testing

4.4.5.1 Introduction - The auditor has two document verification responsibilities. The first is to ensure that the documents are prepared in accordance with the system development methodology. [Note: This may be done by another independent review group, for example, quality assurance, or may be done by the auditor on a test basis.] Second, the auditor wants to ensure that the same information is accurately transferred from document to document to document. The latter responsibility is one that requires the auditor to understand the project, as well as the flow of documents through the development process.

4.4.5.2 Definition Phase Audit Tests - The auditor should validate sufficient attributes of the documentation to enable reliance to be placed on them. At the end of this process, the auditor will need to develop an opinion as to whether or not there are deficiencies in the

project, and to make recommendations. Testing independent sources will permit those recommendations to be developed.

The validation should be performed using the Definition Phase detailed audit testing program. (See Table 4.2) This program contains a set of audit objectives/indicators for evaluation. For each audit objective/indicator that the auditor selects, audit tests are recommended, together with the tools and techniques for performing those tests. The audit program is designed to help the auditor select those items requiring validation.

4.4.5.3 Survey Questionnaire Definition Phase - The documents and the key attributes to be included in each document that the auditor should verify follow. [Note: This information is needed, even if the developmental methodology has a slightly different set of documents.]

1. Project Plan should contain:
   (a) Strategy for managing the software;
   (b) Goals and activities for all phases and subphases;
   (c) Resource estimates for the duration of the system development process;
   (d) Intermediate milestones, including management and technical reviews;
   (e) Methods for system development, documentation, problem reporting, and change control; and
   (f) Supporting techniques and tools.

2. Functional Requirements Document should contain:
   (a) The proposed methods and procedures;
   (b) A summary of improvements;
   (c) A summary of impacts, internal controls, security, and privacy considerations;
   (d) Cost considerations and alternatives;
   (e) The functions required of the software in quantitative and qualitative terms;
   (f) How the software functions will satisfy the performance objectives;
   (g) Performance requirements such as accuracy, validation, timing, and flexibility;
   (h) Explanation of inputs/outputs; and
   (i) The operating environment.

3. Functional Security and Internal Control Requirements Document should contain:
   (a) Vulnerabilities identified during Risk Analysis; and

(b) Established internal control standards, and general as well as application control requirements.

4. Data Requirements Document should contain:
   (a) Data collection requirements (both static and dynamic data);
   (b) Logical groupings of data;
   (c) The type of information required to document the characteristics of each data element;
   (d) Specification of the information to be collected by the user;
   (e) Specification of the information to be collected by the developer;
   (f) Procedures for data collection; and
   (g) Impacts of the data requirement needs.

5. Data Sensitivity/Criticality Description should include:
   (a) Sensitive/critical types of data;
   (b) Sensitive/critical types of assets; and
   (c) Degree of sensitivity of data and assets.

4.4.6 Audit Results/Reporting

At the conclusion of audit testing, the information needed to develop findings and recommendations has been collected. At this point the auditor will need to determine any variances between actual and expected results. For each variance the auditor will need to determine whether that variance is significant, and if so, to develop recommendations.

4.4.6.1 Potential Deficiencies - The objective of the review is to identify deficiencies in the Definition Phase. While the specific deficiencies will vary based on the AIS, there are deficiencies which are common to the Definition Phase. These are listed below in order to help the auditor assure that these deficiencies have not been overlooked in the review:

1. The estimate for resources and time required to implement the system is unrealistic based on the requirements. The auditor might utilize an automated estimating package in order to validate the reasonableness of the estimate.

2. The definition is inadequate to move to the next phase of systems development. If the attributes specified in the documents for this phase are not complete, there is a high probability that extra resources will be required in the following phases to compensate for this deficiency.

3. The input requirements are incomplete. The information needed for processing has not been fully specified, thus making design impractical.

4. The needed output requirements are incomplete. The lack of these requirements will make system design impractical and uneconomical.
5. The processing specifications are incomplete. The definition does not indicate how input requirements will be converted to output requirements. The net result is that extra time will be required during design to develop this definition.

6. The system failures and/or impact of those failures will be inadequately defined. The net result is that the appropriate recovery procedures may not be developed.

7. The level of service needed to achieve the processing objectives will not be adequately defined. The net result is that operations may not have the necessary processing capacity to handle the system requirements.

8. The security and internal control requirements may not be fully defined. The net result is that the implemented system may lack adequate security and internal controls.

9. The assets requiring sensitivity/criticality controls may not be defined, resulting in operational problems due to inadequate handling of the asset.

4.4.6.2 Potential Effects of Deficiencies on Meeting System Mission - Problems inadequately addressed in the Definition Phase will lead to escalating costs throughout the remainder of the system development process. Dr. Barry Boehm in the book Software Economics [BOEMB81] estimated that the cost of fixing inadequate definitions in the operational phase of an AIS could be 100 times as costly as addressing the same problem in definition. Thus, it is critical for the auditor to not only identify the deficiencies, but to estimate the impact of those deficiencies.

The impact of Definition Phase deficiencies can be estimated in one of two ways. First is the actual cost of the deficiency itself. For example, the lack of controls may result in the loss of assets in the operational system. Second, the auditor should estimate the escalating cost of fixing definition problems. The rule of thumb provided by Dr. Boehm is that for each unit of cost estimated as needed to fix a Definition Phase deficiency, it will cost ten times as much by the time the test phase occurs, and 100 times as much once the system is placed into operation.

4.4.7 Reassess Audit Strategy

At each step of the developmental process, the auditors should reassess the audit strategy and level of effort based upon the findings and recommendations during that phase. In addition, during the Definition Phase, the auditors should establish the Audit Plan.

The audit plan should be based upon accomplishing the six audit objectives outlined in the GAO "Yellow Book"[GAO81-1]. These are:

1. Provide reasonable assurance that systems/applications carry out the policies management has prescribed for them.

2. Provide reasonable assurance that systems/applications provide the controls and audit trails needed for management, auditor, and operational review.

3. Provide reasonable assurance to management that systems/applications include the controls necessary to protect against loss or serious error.

4. Provide reasonable assurance that systems/applications will be efficient and economical in operation.

5. Provide reasonable assurance that systems/applications conform with legal requirements.

6. Provide reasonable assurance that systems/applications are documented in a manner that will provide the understanding of the system required for appropriate maintenance and auditing.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	A Project Plan should be developed that specifies the strategy for managing the software/AIS development.	1. Validate that the attributes included within the Project Plan are accurate and complete. 2. Determine that the Plan identifies the strategy for managing the development effort. 3. Determine that the Plan identifies goals and activities for all phases and subphases, and includes milestone dates and resource estimates.	Compare the Project Plan attributes to NBS SP 500-98 and FIPS PUB 102. Use Project Plan checklists included in the system development methodology. Compare the attributes of the Project Plan to other projects of equal size and complexity to validate reasonableness of estimates and milestones.
2.	A definition of existing and new information requirements should be specified with exacting detail.	1. Determine whether the existing and new information requirements are complete and specified in enough detail to permit test data generation in subsequent phases for compliance verification. 2. Interview appropriate user personnel to validate reasonableness of information requirements. Determine the constraints on the data requirements. Indicate the limits of the data requirements with respect to further expansion or utilization, especially emphasizing the constraints that could prove critical during the development process. 3. Validate that the information requirements are complete and consistent with standard data processing definitions.	Verify the information attributes in the Functional Requirements Document to the definitions in the data dictionary.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
2.	(continued)	4. Ascertain if the description of the present system is adequate and serviceable as a basis for studying the needs for the proposed system. Determine if the areas in the present system which would be changed by the proposed system have been clearly identified.	Review audit workpapers of previous audits indicating the attributes of the system being automated or changed. Interview those responsible for operating and maintaining the current system for their perspectives on current problems and the proposed system's impact on the current system and its interface systems.
		5. Include audit tests to ensure that functional requirements as enumerated in Section 4.4.5.3 are considered.	Use items enumerated under the Functional Requirements Document in Section 4.4.5.3 as a checklist.
3.	All input requirements should be defined and documented.	1. Review the adequacy of documentation for input requirements of the new system to ensure they include: a) Editing and validation requirements b) Input or update authorization c) Establishment of appropriate control totals d) Required precision for each quantitative field e) Time requirements for the entry of transactions f) Requirements for handling inaccurate error identification/correction or incomplete data	Validate input requirements specifications to data dictionary specifications. Interview users responsible for data items to confirm accuracy and completeness of input requirements. Validate attributes of data to that specified by appropriate regulations.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)	g) Rules for authorizing each of the key transactions	
		h) Verification that the individuals identified by the authorization rules have been granted that specific authority	
		i) The retention requirements for input data (automated and hard copy) have been specified	
		j) On-line entry application considerations	
		k) Suspense files--verify their use	
		l) System override/by-pass--verify that controls over these transactions are specified and limited	
		m) Describe input forms/transactions/sources/volumes	
		n) Input terminal/device specifications	
		o) Input technology/compatibility	
4.	Output requirements should be defined and documented.	1. Review the adequacy of documentation for output requirements of the new system to ensure that the provisions include such items as:	Interview users to validate the accuracy and completeness of the output requirements.
		a) Content and format of reports and screens generated	User satisfaction questionnaire (GAO "Black Book" [GAO81-3]).

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
4.	(continued)	b) Authorization of users to receive reports c) Retention period of reports d) Provision of audit trails and sufficiency of information to trace/validate accuracy e) Retention periods for outputs (automated and hard copy) f) The ability to ensure control of the completeness, accuracy, and authorization of data g) Purpose of the report	System development methodology review questionnaires (if included as part of the development methodology). If checklists are not provided by the development methodology, the auditor should refer to Appendices G and H to select a manual that provides review checklists and modify them, as appropriate, for review purposes.
5.	Specification for processing steps should be defined and documented.	1. Review processing specifications to determine if they are adequate and were prepared in accordance with management policies, to assure that: a) Cut-off methods have been established b) All computer-generated transactions have been identified c) Appropriate authority exists for generating computer transactions d) Requirements specify method for monitoring the computer-generated transactions	Processing review checklists(if provided by the system development methodology). If checklists are not provided by the development methodology, the auditor should refer to Appendices G and H to select a manual that provides review checklists and modify them, as appropriate, for review purposes. Interview users to validate the accuracy and completeness of the processing specifications. System modeling/prototyping to produce simulated system results for validation by end users of the reasonableness and usefulness of those results in user processing.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
5.	(continued)	e) The methods required for maintaining independent control totals on key fields are reasonable f) Control totals will be support-able and that the transactions comprising the control totals can be identified	
6.	A plan for converting from existing process to new process has been documented.	1. Review conversion plan for: a) Controls during conversion b) Handling of pipeline transactions	Interview key user and data processing personnel to ensure appropriate conversion processes are in place and conform to agency policies and procedures.
7.	The impact of system failures should be defined and reconstruction requirements specified.	1. Determine if a decision has been made about the necessity of recovering the system in the event of failure, and if so, whether the requirements for retention, reconstruction, and/or alternate processing procedures have been defined. 2. Simulated disaster scenario -- Key security personnel/operations personnel can simulate potential disasters and then determine, based on the system specification, whether the available information would be necessary for reconstruction purposes. (Note that in later phases actual disasters can be simulated.)	Interview security officers/operations personnel to determine whether they believe reconstruction requirements are adequate. Determine that the retention period for reconstruction is consistent with retention period specified in appropriate Federal regulations/agency recorded retention programs.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
8.	The level of service necessary to achieve the processing objective should be defined and documented.	1. Determine that: a) A desired percentage of up time has been specified b) The response time for each transaction has been specified c) The needed computer capacity has been specified d) It is reasonable based upon user department needs.	Interview key user personnel to validate that the specified service levels are adequate. Interview key operations personnel to validate that operations can provide the processing necessary to accomplish the desired service levels.
9.	The internal control and security requirements should be defined and documented, per OMB Circular A-130.	1. Determine whether the user requirements include security, control, and privacy issues and then validate that those requirements are adequate and address previously defined risks.	Identify the control techniques needed to minimize vulnerabilities for the proposed system. GAO "Green Book" [GAO83] Compliance with the requirements indicated in FIPS PUBs 38, 64, and 87. GAO "Black Book" [GAO81-3] as guidance to the types of control requirements needed in application systems.
10.	The user requirements should identify critical/sensitive data and assets, and how those items should be controlled during computer processing.	1. Validate that the system requirements indicate the data and asset sensitivity/criticality protection requirements.	Review appropriate legislation (e.g., Privacy Act of 1974, Freedom of Information Act, etc.) in order to validate that the types of transactions/data/assets governed by the system will be adequately protected.

TABLE 4.2 - DEFINITION PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
11.	Audit and quality assurance tools and techniques should be planned for the system.	1. Validate that needed audit and quality assurance tools and techniques are available in the system or, if they are missing, develop requirements for these tools and techniques.	Review appropriate documentation and interview cognizant personnel.
12.	The System Decision Paper should include all of the information needed by user management to make a decision on action to be taken regarding the AIS.	1. Verify there is a consensus among user departments and designers concerning the recommended alternative, the costs/benefits, and the technological aspect of the systems implementation approach.	Structured interview technique.
		2. Determine that the System Decision Paper includes all of the essential information on the AIS, such as: a) Mission need b) Risks c) Alternatives d) Costs/benefits e) Management plan f) Supporting rationale for decisions g) Affordability in terms of projected budget and out-year funding h) Conceptual definitions i) Practicality of implementation plan - SDLC - Team/personnel/resources - Monitoring/oversight j) Consistency with long-range plans and other IRM initiatives	Compare the structure and content of the System Decision Paper to the structure, format, and content of the system decision paper as outlined in FIPS PUB 64.

4.5 AUDIT PARTICIPATION IN THE SYSTEM DESIGN PHASE - PHASE III

The objective of this phase is to develop detailed design specifications which describe the physical solution to the system requirements developed during Phase II, the Definition Phase. The challenge of this phase is to determine how the requirements can be satisfied using the computer. It may also be necessary to resolve deficiencies and clarify particular requirements in more detail so that the computer solution can be finalized and documented.

The audit objective during the system Design Phase is to ensure that system requirements are adequately incorporated into the design specifications. The auditor should concentrate on the adequacy of controls in the design. The auditor also wants to ensure that the system is auditable, and to design the methods for auditing the system once it becomes operational.

4.5.1 Primary Audit Objective fo the System Design Phase

The primary audit objective of the system Design Phase is:

"To ensure that system requirements are adequately incorporated into design specifications, including controls that ensure auditability."

The accomplishment of this objective necessitates that the auditor understand the system design process, as well as the application area and the controls needed to govern that area.

4.5.2 Overview of the System Design Phase

The Initiation and Definition Phases are designed to clarify and document Sponsor/User needs and requirements. The system Design Phase takes those requirements and converts them into specifications for a computerized system. The more specific the requirement specifications, the easier it becomes to develop a workable computer solution. On the other hand, if the requirements are not correctly or fully defined, additional work will need to be done during the Design Phase in order to produce the outputs required by the Sponsor/User to satisfy his/her needs.

The third phase results in a technical specification of the problem solution. The solution provides a specific high-level definition, including information aggregates, information flows and logical processing steps, as well as major interfaces and their inputs and outputs. The purpose is to refine the problem, resolve deficiencies, define additional details and package the solution. The detailed design specifications describe the physical solution (algorithms and data structures) in such a way that it can be implemented in code with little or no need for additional analysis.

[Note: Agencies should define and approve internal control/security specifications prior to acquiring or starting formal development of the applications. This is advisable for generating a suitable system since few data processing professionals have extensive training in design principles and practices, and this weak area of system development needs all the knowledgeable input possible.]

The validation, verification and testing (VV&T) goals are also identified during this phase, and a plan for achieving these goals is developed (see FIPS PUB 101). The system tests should be able to verify that required administrative, technical, and physical safeguards are operationally adequate. The Project Plan (schedules, budgets, deliverables, etc.) and Risk Analysis are reviewed and revised as required, given the scope and complexity of the solution formulated. These activities are coordinated with the Certification Plan components.

4.5.2.1 Participants and Their Tasks - Listed below are the responsible participants in the system Design Phase, with a brief description of their role during the phase:

1. Information Resources Management (IRM) Official - Approves updated System Decision Paper to advance to the system Design Phase, in consultation with Sponsor or User and ADP Manager (occurs between phases), and enters system into department's formal systems inventory.

2. System Security Officer (SSO)/Internal Control Officer (ICO) - Reviews SSO/-ICO components of System/Subsystem, Program and Data Base Specifications, and Validation, Verification and Testing Plan and Specifications.

3. Auditor(OIG) - Reviews/evaluates and possibly provides inputs to Risk Analysis, System Decision Paper, System/Subsystem, Program and Data Base Specifications, VV&T Plan and Specifications, and revised Project Plan; updates Audit Plan.

4. Sponsor/User - Approves revised Project Plan and updates System Decision Paper; reassesses Risk Analysis; approves Validation, Verification and Testing Plan and Specifications (all based on QA recommendations, where available).

5. Project Manager/Contracting Officer's Technical Representative (COTR) - Updates Project Plan; develops System/Subsystem, Program and Data Base Specifications, and Validation, Verification and Testing Plan and Specifications.

6. System Security Specialist/Internal Control Specialist - Reviews SSO/ICO components of System/Subsystem, Program and Data Base Specifications and Validation, Verification, and Testing Plan and Specifications.

7. Contracting Officer - If appropriate, awards contract.

8. Contract Auditor - If appropriate, assures contract compliance.

9. ADP Manager - Reviews VV&T components of System/Subsystem, Program and Data Base Specifications, and VV&T Plan and Specifications; as appropriate, provides technical support to Project Manager and Sponsor/User.

10. Quality Assurance (QA) Specialist - Reviews system design, VV&T components, and documentation for compliance to definition and data processing standards.

4.5.2.2 System Design Phase Documents - During the system Design Phase, three new documents will be created and three documents will be updated, all based on the work done during the Design Phase.

The three new documents are:

1. System/Subsystem, Program and Data Base Specifications (FIPS PUB 38) - The purpose of the System/Subsystem Specifications is to specify the requirements, operating environment, design characteristics, and program specifications. The purpose of the Program Specifications is to specify the requirements, operating environment, and design characteristics of a computer program. The purpose of the Data Base Specifications is to specify the nature, logical and physical characteristics of a particular data base. [Note: These may actually be three separate documents.]

2. Security and Internal Control Related Specifications (FIPS PUBS 73 & 102) - The purpose is to set forth security and internal control specifications to meet the functional security and internal control requirements. This document may be included as an appendix to System/Subsystem, Program and Data Base Specifications document.

3. Validation, Verification, and Testing Plan and Specifications (FIPS PUB 101) - The purpose of the VV&T Plan is to plan for the evaluation of quality and correctness of the software, including requirements and design documentation. The VV&T Plan also contains plans for the testing of software, including detailed program specifications, descriptions, internal contols and security specifications, and procedures for all tests, as well as test data reduction and evaluation criteria.

The three updated documents are:

1. Audit Plan
2. Project Plan
3. System Decision Paper

4.5.3 Audit Survey

The extent of the background work to be performed by the auditor will depend upon his/her participation in the earlier phases, as well as the project status as perceived by the auditor at the conclusion of the previous phase. The better the understanding the auditor has of the system, or the better controlled the system, the less preparatory work the auditor will need to do for this phase. The four tasks that the auditor will need to perform are:

1. Review Definition Phase outputs;
2. Review Design Phase plans;
3. Review information on Design Phase status; and
4. Verify information on Design Phase status.

Note that the specific work within these four tasks will be dependent upon the customized audit objectives selected for this phase (reference Section 4.5.4). These four tasks are individually discussed below:

4.5.3.1 Review Definition Phase Outputs - Prior to beginning the survey phase of project design, the auditor should study the results of the Definition Phase review. This would include reviewing any workpapers and reports prepared by the audit review of the Definition Phase, plus the key documents produced during the Definition Phase. It is also good practice to reread Section 4.4 on Definition Phase audit before reviewing the results of the Definition Phase, to reorient the auditor to the documents that are normally produced during that phase, and the types of customized audit objectives and work programs that are performed by the auditor during the Definition Phase.

4.5.3.2 Review Design Phase Plans - The Project Manager should prepare and maintain a Project Plan. This document would contain a work plan, schedule, budget, individual assignments, and work tasks to be performed by the project team. The auditor should review this to determine what work products are to be produced during this phase, the sequence in which those work documents will be produced, to whom the task of preparing the documents have been assigned, and the schedule and effort associated with each of the work documents. This will enable the auditor to know the sequencing and scheduling of work documents so that the auditor can develop an appropriate audit work schedule.

4.5.3.3 Gather Information on Design Phase Status - The auditor should gather the documents appropriate to the design methodology. The type of documents that the auditor needs to obtain and review during the background step of the Design Phase audit are:

1. System/Subsystem, Program, and Data Base Specifications;
2. Security and Internal Control Specifications;
3. Validation, Verification, and Test Plan and Specifications;
4. Updated Risk Analysis;
5. System Decision Paper (including updated cost/benefit data and analysis); and
6. Updated Project Plan.

The auditor needs to gather information about the status of the above documents. Specifically, the auditor should determine:

1. Status of document - Are they complete? If not, is additional work planned to be undertaken to complete the documents, and if so, when will they be done?

2. Has the project proceeded according to the Project Plan? - If not, what action is being taken to get the project back on target?

3. Have any changes been made to the project's functionality or architecture? If so, the auditor needs to assess how they may impact the customized audit objectives for previous audit phases and this phase.

4.5.3.4 Verify Information on Design Phase Status - The work done to verify the information on Design Phase status will be based upon the customized audit objectives selected.

4.5.3.4.1 Review Documents - The flow of work will depend upon the specific system development methodology being used. Figure 2 represents the more traditional flow of paperwork in the SDLC and includes the Design Phase. This figure shows the input from the previous phase, the documents and document updates produced during this phase, and the sequence in which they are produced.

For many data base systems, prototype systems, and skeletal code systems, programming commences immediately after the Definition Phase. About the only parts of the identified Design Phase documents that the auditor could expect to find are:

1. Operating environment, design characteristics, and program specification parts of the System/Subsystem, Program and Data Base Specifications.

2. Security specification part of the Security and Internal Control Related Specifications. [Note: While internal controls are very important, they may not be included in this document because the control portion may not have been deemed necessary in the initial prototype version. This decision to develop without controls contains serious risks since the subsequent inclusion of controls may introduce major alterations in system behavior and cost.]

In the newer developmental methodologies, the Sponsor/User may do the testing himself/herself by examining the output to determine if it meets needs. If, however, the system must fulfill a significant business/organization function, then the auditor should expect to find at least a minimal test plan, regardless of the type of developmental methodology.

4.5.3.4.2 Interview the Participants - The role of the responsible participants will also vary depending on the system development methodology. For example, in prototyping, the Sponsor/User has a very active role in working with the developers through an iterative process of design and implementation.

The auditor is concerned first that the proper responsible participants are included in the system Design Phase, and second that they perform their proper roles. Again, note that the names used for responsible participants may vary from agency to agency. What the auditor must do, if the individuals listed here are not involved, is to determine whether or not the functions are performed, and if so, is there adequate division of responsibilities to ensure the necessary checks and balances for an effective system design.

The questions that the auditors should ask of the responsible participants include:

1. Information Resources Management (IRM) Official
   (a) Has the System Decision Paper been approved?
   (b) Has the system been entered into the department's formal system inventory?

2. System Security Officer/Internal Control Officer
   (a) Have the SSO/ICO components of the system/subsystem been reviewed?
   (b) Have the SSO/ICO components of the Program and Data Base Specifications been reviewed?
   (c) Have the SSO/ICO components of the Validation, Verification, and Testing Plan and Specifications been reviewed?

3. Sponsor/User
   (a) Has the revised Project Plan and updated System Decision Paper been approved?

(b) Has the Risk Analysis been reassessed?
(c) Has the Validation, Verification, and Testing Plan and Specifications been approved?

4. Project Manager/Contracting Officer's Technical Representative (COTR)
   (a) Has the Project Plan been updated?
   (b) Have the System/Subsystem, Program and Data Base Specifications been developed?
   (c) Have the Validation, Verification, and Testing Plan and Specifications been developed?

5. System Security Specialist/Internal Control Specialist
   (a) Have the SSO/ICO components of system/subsystem been reviewed?
   (b) Have the SSO/ICO components of the data base specifications been reviewed?
   (c) Have the SSO/ICO components of the Validation, Verification, and Testing Plan and Specifications been reviewed?

6. Contracting Officer
   (a) Has the Contracting Officer, if appropriate, awarded the contract?

7. Contract Auditor
   (a) Has the Contract Auditor, if appropriate, assured contract compliance?

8. ADP Manager
   (a) Have the VV&T components of the system/subsystem been reviewed?
   (b) Have the VV&T components of the Program and Data Base Specifications been reviewed?
   (c) Have the VV&T Plan and Specifications been reviewed?
   (d) Has technical support been provided to the Project Manager and Sponsor/User, if required?

9. Quality Assurance Specialist
   (a) Have the system design, VV&T components, and documentation been reviewed for compliance to definition and data processing standards?

4.5.4 Customize Audit Objectives

The audit objectives established for each AIS will vary depending upon (1) the purpose, objective, and scope of the application, and (2) the auditor's concern over the ability of the project team to successfully complete the project. This section offers a standard set of audit

objectives/indicators for use by the review team. However, this list will need to be customized by the audit team, based upon their assessment of the AIS under review.

4.5.4.1 Design Methodology Audit Considerations - The auditor may encounter significantly different design methodologies from agency to agency and system to system. While the Initiation and Definition Phase of system development remain fairly constant, there are many different methodologies for designing computer systems. Among the more common approaches (which can be used singly or in combination) are:

1. Life cycle oriented design methodologies - The organization of this manual is oriented toward the life cycle design methodology. In this concept, there are distinct phases during which the design evolves. Each phase is distinct, producing deliverables (i.e., products) which are input to the next phase.

2. Structured design methodologies - These are similar to the phase design methodologies, except the documents produced are different. The structured design methodologies usually use Warnier-Orr diagrams to graphically illustrate the logic paths throughout the design structure.

3. Data base management systems - The significant difference between data base and non-data base is the responsibility for data design. In data base systems, data design is performed by data base administrators, and the utilization of that data requires a new series of documents.

4. Skeletal code - This is a design concept normally oriented toward a data base structure. The key design concept is the partial construction of programs. In many instances, one half or more of the program will be precoded in a generalized or skeletal format. The designers can pick and choose among these skeletal programs for use in meeting Sponsor/User needs. In addition to the skeletal code, the designers may choose utility programs, general-purpose programs such as data retrieval and analysis or report generators, as well as languages provided by data base and data communication software.

5. Prototyping - Prototyping is one of the newer design concepts which incorporates two new design principles. The first is an interactive design process. Prototyping recognizes that it is very difficult to define requirements correctly the first time. Therefore, prototyping produces a system as quickly as possible so that the Sponsor/User can determine whether or not it meets needs. If it does not, the prototyping process continues until the right system has been designed. The second characteristic of prototyping is the collapsing of system development phases.

After basic requirements are done, the system design and remaining phases are normally collapsed into a single phase.

The auditor must first determine what design methodology is used, and then learn the functional aspects of that design methodology. The documents identified in this audit guide may vary significantly in this phase from what the system design group actually produces. For example, if prototyping or skeletal code is used, then much of the information contained in the system design documents described in this audit guide may not be necessary.

When the auditor encounters an unusual design methodology, the auditor should:

1. Reconcile the design methodology to the life cycle development methodology described in this audit guide. If the same basic information is produced, then the audit programs outlined in this audit guide are applicable. The auditor need only customize the audit approach to the specific design methodology.

If the auditor cannot reconcile the actual design methodology to the one imbedded in this audit guide, then the auditor should:

2. Study the design methodology sufficiently to see how the life cycle phases in this audit guide are collapsed by the methodology and regroup the audit programs to conform to this condensed life cycle. It would then be a matter of judgement to decide what parts of the audit programs are applicable to this situation.

4.5.4.2 Contracting/Purchase Audit Considerations - There will be significant differences in the audit involvement in this phase if the software is contracted or purchased rather than developed in-house. For contracted software the auditor may: (1) interface with contractors; (2) be involved in evaluating requests for bid and analysis of those bids; and (3) be involved in the selection of contractors from an audit perspective. If the software is purchased off-the-shelf, then the auditor may be involved in that purchase to ensure that the acquired software meets the requirements established in the previous phase.

For contracted software, the Project Manager or the Information Resources Management Official oversees the project during this phase to ensure objectivity of results and to preclude conflicts of interest between project goals and contractor expediency. The Auditor then oversees this activity to ensure its effectiveness.

For off-the-shelf software, the Sponsor/User reviews the proposed procurement for sufficiency; the Project Manager identifies and appoints a technical evaluation panel to review technical competency of bids/offers; and the ADP Manager reviews requirements documents as well as provides technical assistance to the Contracting Officer relative to development of

the procurement action. The Auditor then assures that all these activities have taken place and with appropriate care.

For software that has been purchased or contracted, the auditor should address the following specific points:

1. Has the contract been prepared in accordance with government purchasing requirements?

2. Does the contract provide for audit review of the contractor/developer work?

3. If the contractor goes out of business, does the government obtain source code for the software (in the case where the contractor does not provide original source code)?

4. Does the contractor/developer have appropriate controls and safeguards to assure the quality of the software being produced (e.g., a quality assurance function, a detailed testing methodology)?

5. Does the contract provide for maintenance of the software?

6. Does the contractor/vendor have a test plan?

7. Does the contractor/vendor develop essentially the same documents as defined in this audit guide?

4.5.5 Detailed Audit Testing

4.5.5.1 Introduction - During the detailed audit testing, the auditor needs to concentrate on the three new documents created during the Design Phase, not, however, to the exclusion of the three updated documents. The auditor should be concerned that the updated documents correctly reflect changes made in the areas covered by those documents during the Design Phase. The amount of validation that the auditor will do on both the new and updated documents will be dependent upon the degree of risk associated with the application system. The greater the risk, the more extensive the validation.

4.5.5.2 System Design Phase Audit Test Program - The following system Design Phase audit program is a program for validating the Design Phase documents. This program is audit objective driven. For each objective to be accomplished during validation, the auditor is provided with a series of tests to perform. For each test, some tools and techniques are recom-

mended. Note that in this phase, automated tools are proposed, but the use of these will be dependent upon their availability at the installation where the review occurs. (See Table 4.3)

In designing an audit program for the system Design Phase, the auditor should read FIPS PUB 101. That document provides guidance on validating system Design Phase products. While the publication was developed for data processing personnel, the validation insight in the document is equally helpful to the auditor in preparing for and executing a system Design Phase review.

4.5.5.3 Survey Questionnaire Design Phase - The document verification process requires the auditor to examine the documents to ensure they are complete, reasonable, and consistent between documents. Verification can best be done by using a checklist provided with the system design methodology. However, if verification has already been performed by data processing, quality assurance, or a project review team, the auditor may want to ensure the quality of the designer's work and, if it is determined to be satisfactory, then perform the validation step.

Questions to ask for each document include:

1. System/Subsystem, Program, and Data Base Specifications

   (a) Does the document specify the design requirements?
   (b) Does the document specify the operating environment?
   (c) Does the document specify the design characteristics?
   (d) Does the document specify the program requirements?
   (e) Does the document specify the program operating environment?
   (f) Does the document specify the program design characteristics?
   (g) Does the document describe the functions and performance requirements?
   (h) If so, are these performance requirements described in terms of accuracy, validation, timing and flexibility, and also the operating environment?
   (i) Is the nature, logical, and physical characteristics of data bases used specified?
   (j) Does the Data Base Specification address storage and design considerations?

2. Security and Internal Control Related Specifications

   (a) Does the document specify the security design?
   (b) Does the document specify the internal control design?
   (c) Does the security design meet the security requirements?

(d) Does the internal control design meet the internal control requirements?
(e) Are the security and internal control specifications in sufficient detail so that tests can be designed that will tell whether requirements are satisfied?
(f) Are changes to the system evaluated to determine whether they impact internal control or security design?
(g) If so, is internal control and security design changed accordingly?
(h) If this is a sensitive application, has it been reviewed and approved by the party responsible for security and control?

3. Validation, Verification, and Testing Plan and Specifications

(a) Does the document include a plan for testing the software?
(b) Does the plan include detailed specifications, descriptions, and procedures for testing all systems?
(c) Does the test plan include test data reduction and evaluation criteria?
(d) Is the VV&T Plan related to the system plan?
(e) Does the system plan drive the VV&T Plan?
(f) Does the VV&T Plan include general project background and information on the proposed solution to the mission deficiency(ies)?
(g) Does the VV&T Plan include VV&T requirements, measurement criteria, and constraints?
(h) Does the VV&T Plan include procedures to be applied during development in general and by phase?
(i) Does the VV&T Plan include supporting information for VV&T selections made?
(j) Does this document include appendices which describe project and environmental considerations?
(k) Does this document include appendices which define the testing technique and tool selection information?

4.5.6 Audit Results/Reporting

The results of testing need to be analyzed, conclusions and recommendations developed, and that information presented to the auditee in report format. The report should identify the potential deficiencies, indicate the potential effect of those deficiencies on meeting the systems mission, and then present recommendations to overcome those deficiencies.

4.5.6.1 Potential Deficiencies - The deficiencies found will vary from application to application. However, experience has shown that certain deficiencies are common in the Design Phase, and, if these deficiencies are not corrected, serious application problems will occur

during implementation. The following eight deficiencies are listed to assist the auditor in assuring that the types of deficiencies common to design have not been overlooked in this review:

1. System design documents will not be prepared, or not prepared in accordance with the document intent.

2. The system of internal control will not be fully developed.

3. The security procedures designed to protect the application will not be fully developed.

4. Needed transactions for processing application information will not be defined, and/or the authorization rules for transactions will not be defined.

5. The audit trail that permits reconstruction of processing will be incomplete.

6. An application vulnerability assessment will not be performed, or performed inadequately, so that all major potential vulnerabilities may not have been identified, and thus the system design is incomplete.

7. The system as designed will not meet the true Sponsor/User needs, and the Sponsor/User will not have had the opportunity to review the design documents and comment on the inadequacy.

8. The phase will be concluded without the Validation, Verification, and Testing Plan being completed.

4.5.6.2 Potential Effects of Deficiencies on Meeting System Mission - At the conclusion of the Design Phase, both the functional and structural aspects of the AIS have been established. If the design has been done correctly, the following phases need only follow that design and the system's mission should be accomplished. On the other hand, if the design is deficient, then an inadequate system might be implemented with potentially disastrous results.

The effect of design deficiencies is twofold. First, they will impact on the implementation, which will cause resources to be improperly utilized. Data processing personnel will be implementing the wrong system, and when it is uncovered will have to take out those incorrectly implemented portions and redesign and reimplement the system. The cost of doing this rework can exceed the original cost of implementation, and frequently does.

The secondary effects of design deficiencies are on the users of the AIS. Unless the deficiencies are caught in the Programming and Training Phase, or in the Evaluation and Ac-

ceptance Phase, they will result in incorrect or incomplete processing. The result can be financial loss, or it can be lost opportunities to effectively perform the agency's mission in accordance with the intent of legislation.

4.5.7 Reassess Audit Strategy

The audit strategy needs to be continually reviewed as the system progresses through the developmental phases. The auditor will be looking at three aspects of audit strategy in the Design Phase as follows:

1. Reevaluate auditor's role in the design - The auditor needs to continually assess whether more or less audit effort is needed during design. If the system is progressing according to realistic schedules and budgets, and the implementation reflects the approved decisions of the previous phase, the amount of audit involvement can potentially be reduced. On the other hand, as the number of uncovered vulnerabilities increases, the greater the need for more audit involvement. In particular, internal control or security weaknesses signify a need for greater audit involvement.

2. Ensure auditability of system - The auditor wants to ensure that the architecture/structure of the system provides the necessary features to make the system auditable. Reviewing the audit objectives for the Design Phase basically satisfies this aspect of audit strategy. For example, if the systems of control are adequate, if there is an adequate audit trail, and if that trail is saved for a reasonable time, then the system is normally auditable. As there are deficiencies in these areas, the system becomes less auditable and the greater the need for a specific audit recommendation to improve auditability.

3. Development of audit programs for the finished application - As the system designers are designing the system, the auditors should be designing how the system will be audited once it goes into production. This means the design of audit programs, and the design/ acquisition of any audit tools necessary to perform that audit. For example, the auditor may want to develop a skeletal extract program which can then be customized for specific transactions or may want to have an integrated test facility included in the system during development.

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	The revised Project Plan is current and provides the direction needed to effectively and efficiently manage the project.	Confirm with the Project Manager that the plan is up to date, is being followed, and provides adequate information to adjust project direction as appropriate to ensure the project will be completed on time, within budget, and produce the expected deliverables.	Compare the status of completed documents to document status as included in the Project Plan. Verify that the plan is accurate, and then, through interview with the document developers, ensure that problems in their work are appropriately addressed by project management.
2.	The final system design should be approved by all appropriate levels of manage- ment as meeting all predetermined needs.	Determine that user department management, and other appropriate management, have reviewed the system design specifications/documents. Confirm that user department management has approved the design as meeting their needs.	Manual examination of evidence indicating that the material has been reviewed (e.g., reviewing minutes of meeting, department memorandum, departmental time sheets, etc.). Examine user "signoff" of design phase documents. System development scheduling software -- Obtain status information from the scheduling packages.
3.	Sufficient data processing and security controls should be incorporated in the detailed design to ensure the integrity of the system.	Review the detailed design specifications and identify the system controls to be built in the system to evaluate the adequacy of those controls. (Note: If control documentation does not exist within the system design documents, this can be an extremely time-consuming task for the auditor.)	Risk points are where controls should be placed. The auditor has a variety of strategies available to identify risk points. The adequacy of controls should be addressed at those points. If the system has been designed using structured design, then the nodes in the structure indicate the points where controls should be exercised. The auditor can use the structured design to show the data flow in the points where data should be controlled. The controls can be documented on the

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)	The areas to be addressed are: 1. How are the controls specified in requirements designed into system? 2. What new risks does design introduce and what controls reduce risk? 3. What mechanisms have been designed to ensure ongoing integrity (e.g., exception reports, control total comparisons)? 4. What are the access control mechanisms?	structured design, with the absence of control at the nodes of the structure indicating potential control weakness. If controls are not documented, and the system is not designed using a structured method, then the auditor has the option of selecting one or more of the control design methodologies available either through the private or public sector. Among the most common are: ● "Black Book" [GAO81-3] -- issued by the GAO ● Auditing Computer Applications --issued by AUERBACH and based on the GAO "Black Book" ● Control matrix analysis -- available through Touche Ross & Co. and described in their book Computer Control and Audit by Mair, Wood, and Davis ● Transaction flow auditing -- materials available through Arthur Andersen and Company If emphasis is on the security part of control, then FIPS PUB 65 should be referenced as a

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	(continued)		security assessment methodology, and NBS SP 500-133 for other methods.
4.	Rules for authorizing transac-tions should be defined and documented.	Determine that the method for authorizing each transaction has been documented, and that the method is reasonable. (Note that the audit process for this will vary depending on whether the transaction originates on paper, or whether it originates electronically.)	For paper transactions, use a structured interview technique to validate that all transactions have been identified, and that the rules for authorizing those transactions are defined. Note that, for financial systems, the financial officer of the agency should be the individual indicating how financial transactions are authorized. For automated transactions, the auditor would need to use the structured interviewing techniques to ensure that all the electronically originated transactions have been identified. The assessment over the controls for authorization is normally implemented through security access packages. The auditor should validate that those security software packages, or equivalent, will be used to validate the authorization of transactions.
5.	Documentation suitable for use as audit trails should be incorporated into the detailed design.	Verify that the audit trail specifications include both the manual and automated segments, and that the audit trail is adequate to trace transactions from point of origin (source documents) to control totals, and from control totals back to supporting transactions.	The auditor should prepare a document flow diagram (see GAO "Black Book" [GAO81-3] for a document flow diagram example). The objective of the document flow diagram is to pictorially show the flow of documents, including electronic documents, who is responsible for those documents, and where the documents are stored. The specific audit trail would be illustrated through notation on the document flow

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
5.	(continued)		diagram, and references to the specific documents, both manual and electronic.
		Determine whether sufficient generations of the documentation will be stored away from the primary site, so that processing can be reconstructed if the primary site is destroyed. Also, validate that the documentation will be retained for the correct retention period based on Federal programs, regulations, and agency policy.	Review of computer operations prepared Disaster Plan. This plan will indicate what documents are to be stored away from the primary site, where they will be stored, and the length of storage. The plan should also indicate how and when the disaster procedures have been tested to validate that they work. Use structured interview technique to identify correct retention periods and compare that to system documentation.
6.	A vulnerability assessment should be planned and performed in compliance with OMB Circulars A-123 and A-130.	1. Determine that a vulnerability assessment has been planned, performed, and documented. 2. Review the vulnerability assessment for reasonableness.	Use structured interview technique to validate with involved parties (refer to identified responsible participant for security) the completeness of the vulnerability assessment.
7.	The system/subsystem, pro-gram and data base specifications should provide the correct architectural solution to meet the documented requirements from the definition phase.	Ensure that the documented system solution will provide the information needed to meet the objectives defined in the previous phases. Review the System/Subsystem, Program, and Data Base Specifications document contents, as indicated in Section 4.5.5.3. [For additional questions, see DOL87, pp.IV-93 to 100.]	Technical peer review group -- A team of peers can be established to review the design to ensure that it meets the system requirements. Note that the auditor may be a member of that review team, with specific responsibilities for the adequacy of the design of the system of internal controls and security procedures. Use the System/Subsystem, Program, and Data Base

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
7.	(continued)		Specifications document concerns, enumerated in Section 4.5.5.3, as a checklist.
8.	The security and internal con-trol related specifications should provide controls adequate for satisfying the control requirements defined in the previous phase.	Ensure that the documented Security and Internal Control Specifications satisfy the controls defined in the previous phase.	Use the items enumerated under the Security and Internal Control Related Specifications document, in Section 4.5.5.3, as a checklist.
9.	A Validation, Verification, and Testing Plan should be developed and documented.	Review the Validation, Verification, and Testing Plan and Specifications to ensure that it includes all of the important parts, as specified in Section 4.5.5.3. Verify that the Test Plan adequately validates the system requirements defined in the previous phase.	Compare the information included within the test plan against one of the following five Test Plan standards and guides: ● GAO "Black Book" [GAO81-3] ● FIPS PUB 38 -- test plan part ● IEEE system test plan standard, and unit test plan standard ● AUERBACH guidance for software testing ● FIPS PUB 101, VV&T Test Plan Prepare a function/test matrix. This matrix is specified in FIPS PUB 38, and, if included within the documentation, the auditor need only ensure that the function/test matrix is complete. This matrix lists all of the application functions (i.e., requirements) on one axis of the matrix and then cross-references it to all of the tests included in

TABLE 4.3 - SYSTEM DESIGN PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
			the Test Plan. This provides proof that the Test Plan is complete.
10.	Assure that audit and quality assurance tools and techniques have been included in systems design documents.	Validate that the needed audit and quality assurance tools and techniques have been included in the system as it is designed.	Review appropriate documentation and interview cognizant personnel.
11.	Assure that the system design has optimized the use of technology.	Validate that the design effectively uses technology and that adequate controls are incorporated into the design to control technology.	Compare the technology controls against the controls for technology in the appropriate part of the GAO "Black Book" [GAO81-3]. Determine that the Test Plan for the application includes adequate tests of technology. Refer to FIPS PUB 101 for technological test recommendations. (Note: If the auditor does not feel qualified to evaluate technology, consideration should be given to engaging a consultant to evaluate the effective use of technology.)
12.	Ensure that the system decision continues to be supported by documents.	Ensure that the System Decision Paper has been updated.	Obtain and review a copy of the updated System Decision Paper or its equivalent.

4.6 AUDIT PARTICIPATION IN THE PROGRAMMING AND TRAINING PHASE - PHASE IV

During this phase, programs will be developed and tested. The implemented programs should be based on the detailed design/program specifications prepared in Phase III. If the design was well specified, this phase will not be technically difficult, but if there are gaps in the specifications, this phase will be required to compensate for those gaps because programming is very detailed and requires all decisions to be made before the code can be written.

4.6.1 Primary Audit Objective of the Programming and Training Phase

During this phase, but prior to approval of the System Decision Paper by management, the auditor should accomplish these two primary objectives:

"1. Ensure that the program/system fully implements the design specifications.
2. Ensure that documentation and training provide for a usable and maintainable system."

The auditor will accomplish these objectives through an evaluation of the Programming and Training Phase documentation. In order to do this, the auditor must understand the system development methodology, the documents that are produced by that methodology, and the flow in which the documents are produced. The auditor must also understand the status of the data processing training program.

The documents produced during this phase will vary from methodology to methodology. Even the same methodology may be implemented differently between two or more agencies and thus produce different documents. In addition, if the software is contracted or purchased, the documents within this phase will change dramatically. Also, as discussed in the Design Phase, if the newer design concepts are used, such as prototyping, the programming part of this phase may not exist and the training aspect may be significantly reduced.

4.6.2 Overview of the Programming and Training Phase

Programming is the process of implementing the detailed design specifications into code. The process of converting specifications to executable code is primarily dependent upon the completeness and specificity of the program design. If the program is well defined, the process of programming is not technically complex.

Most system development methodologies clearly define how systems move from the design to the programming phase. In fact, most data processing professionals are well trained in programming, but few have extensive training in design principles and practices. Thus, from

a technical perspective, programming is frequently the best specified, and the most mastered skill.

Although training is associated primarily with the Programming and Training Phase, the origins of training should commence earlier as a requirement. Training is a specialty, but much of the success of the system will be directly attributable to how well the users are trained. For those parts of the system which they do not understand well, the probability exists that the users will not use those features, or will use them incorrectly. Both impediments to a successful system can be overcome through the proper development and use of training materials.

Training is often excluded from the system development methodologies. Where it is included, it usually does not adequately address specific training requirements. Therefore, the auditor might find a very strong developmental methodology for programming but a very weak methodology for training.

Besides Programming and Training, User and Maintenance Manuals are prepared during the fourth phase (see FIPS PUBS 38 and 64), as is a preliminary Installation Plan which specifies the approach to, and details of, the installation of the AIS. This phase results in programs which are ready for testing, evaluation, certification, and installation.

4.6.2.1 Participants and Their Tasks - The Programming and Training Phase involves all of the same participants that were in the Design Phase. However, the project planners may assign different people to the Programming and Training Phase than they did for the previous phases.

The responsible participants and their functions during this phase are:

1. Information Resources Management (IRM) Official - Approves updated System Decision Paper to advance to Phase IV, in consultation with Sponsor and ADP Manager (occurs between phases).

2. System Security Officer (SSO)/Internal Control Officer (ICO) - Reviews SSO/ICO components of User Manual, Operations/Maintenance Manual, Installation and Conversion Plan, and revised VV&T Plan and Specifications.

3. Auditor - Reviews/evaluates revised Project Plan, System Decision Paper, Validation, Verification and Testing Plan and Specifications, User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan; updates Audit Plan.

4. Sponsor/User - Approves revised Project Plan, revised VV&T Plan and Specifications, User Manual, Operations/Maintenance Manual and Installation and Conversion Plan; updates Systems Decision Paper; initiates user training.

5. Project Manager/Contracting Officer's Technical Representative (COTR) - Updates Project Plan; revises VV&T Plan and Specifications; develops User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan. Project Manager is responsible for programming and testing.

6. System Security Specialists/Internal Control Specialist - Reviews SSO/ICO components of User Manual, Operations/Maintenance Manual, Installation and Conversion Plan, and revised VV&T Plan and Specifications.

7. Contracting Officer - If appropriate, awards contract.

8. Contract Auditor - If appropriate, assures contract compliance.

9. ADP Manager - Reviews VV&T relevant parts of User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan; provides technical support to Project Manager and Sponsor/User; may conduct training.

10. Quality Assurance Specialist (QA) - Reviews program definition, program code, documentation, and training, for compliance to design and data processing standards.

4.6.2.2 Programming and Training Phase Documents - There are three new documents produced during this phase:

1. User Manual (FIPS PUB 38, DOD-STD-7935, OMB A-130, OMB A-123) The purpose of the User Manual is to sufficiently describe the functions performed by the software in non-ADP terminology, such that the user organization can determine its applicability, as well as when and how to use it.

2. Operations/Maintenance Manual (FIPS PUBS 38 & 106, DOD-STD-7935, OMB A-130, OMB A-123) Two separate manuals may be necessary. The purpose of the Operations Manual is to provide computer operations personnel with a description of the software and the operational environment so that the software can be run. The purpose of the Program Maintenance Manual is to provide the maintenance programmer with the information and source code necessary to understand the programs, their operating environment, and their maintenance procedures and security requirements.

3. Installation and Conversion Plan (FIPS PUB 101, "Implementation Procedures" DOD-STD 7935, OMB A-130, NBS SP 500-105) The Implementation Procedures are a tool for directing the installation or implementation of an AIS at locations other than the test site. This tool is used after testing of the AIS, including security and internal control features, has been completed.

4.6.3 Audit Survey

The Programming and Training Phase implements the system design. The auditor will have two challenges during this review. The first is to ensure that the implementation is consistent with the design; the second is to review the controls over changes. The survey will provide the auditor the background necessary to accomplish these tasks.

4.6.3.1 Review System Design Phase Outputs - As the life cycle progresses, the size and detail contained in the system documents increases. The design document review will be significantly more time consuming than the Initiation and Definition Phase document review. For that reason it is important for the auditor to focus the review on the key elements of those documents.

The auditor should concentrate the review on (1)the Security and Internal Control Related Specifications, and (2)the Validation, Verification, and Testing Plan and Specifications. The role of the auditor, as defined in GAO's audit standards, is heavily directed toward assessing the adequacy of internal controls and security controls. In order to do this, the auditor must understand the design specifications for those controls. Thus, in reviewing the Programming and Training Phase, the auditor should concentrate on the adequacy of internal controls and security controls.

In the evaluation of internal controls and security, the auditor has three activities to perform. The first is to identify the magnitude of the risk facing the AIS. Second, the auditor must determine what security controls and other internal controls are in place. The third activity is to determine whether the controls work. Based on these three activities, the auditor makes an assessment as to whether the working controls are adequate to reduce the risk to an acceptable level. The auditor's opinion is based on this assessment.

The Validation, Verification, and Testing Plan provides the standards against which implementation will be measured. This plan defines the test conditions that will validate controls. This document will indicate how the project team plans to implement the controls. Assuming that the auditor has reviewed these documents, the two define precisely how the controls should be implemented, and thus provide the guidelines for conducting the programming review.

Training is an essential aspect of the proper performance of the operational AIS. The auditor's concern in training is that the controls will be properly exercised. Thus, the analysis of the previously discussed two documents provides the background the auditor needs for evaluating training in the use of internal controls and security controls.

4.6.3.2 Review Programming and Training Phase Plans - Project teams which have firm implementation dates for AISs may need to make implementation compromises in order to meet those dates. If the project is late going into the Programming and Training Phase, the auditor could expect many of those compromises to occur. Two areas frequently compromised are implementation of internal and security controls (including documentation), and development of training programs. The elimination or curtailment of either or both of these areas may not directly impact the functional correctness of system outputs. In other words, the system may be able to produce the desired reports yet not in a controlled manner, or in an environment in which the users are trained. It is the intent of many project teams to install these areas after implementation.

The auditor wants to ensure that the Project Plan is sufficient to guarantee that controls and training are adequately implemented. The plan should indicate who is responsible for these areas, and how they are to be implemented through specific documents. In reviewing the plan, the auditor will want to assure that the necessary control and training documents are included in the plan, and that there is sufficient time and resources to accomplish them.

4.6.3.3 Gather Information on Programming and Training Phase Status - Controlling system change is particularly troublesome during the Programming and Training Phase. It is during this phase that items are implemented on a very detailed level. Since a computer works in a binary mode, performing one event or another, there is no room for vague implementation. Thus, there are normally many clarifications of design during programming. The auditor wants to ensure that these changes are received, logged, controlled, and implemented in an orderly manner.

The auditor should be particularly concerned, during implementation, about documents either not being produced, or being improperly or partially produced. The review of this phase's status should look not only at the status of the project, but at the status of the completed documents. Again, the auditor should be alert to the fact that if the project falls behind schedule, there is a strong tendency in many projects to delete the nonessential aspects of design, at least the project's view of nonessential documents, in order to meet the implementation date.

The auditor should gather the following six documents during the Programming and Training Phase:

1. System Decision Paper (updated)

2. Project Plan (updated)

3. Validation, Verification and Testing Plan and Specifications (updated)

4. User Manual

5. Operations/Maintenance Manual

6. Installation and Conversion Plan

Note that in different methodologies the same information may be in different documents. If the auditor is involved near the end of the phase, all of these documents should have been produced. If the auditor reviews throughout the phase, then he/she may be able to get the documents and perform the review at the point those documents are prepared.

4.6.3.4 Verify Information on Programming and Testing Phase Status - The auditor should be looking for two general areas in verifying status. First, that internal controls and security controls are properly implemented, and second, that all of the design specifications are implemented.

4.6.3.4.1 Review Documents - The flow of work must be compared against the system development methodology in use. If other documents are produced, they should be included and if indicated documents are not produced or updated, that, too, should be noted. Where documents are not produced or updated, it is normally indicative of a potential problem in the application design.

Verification requires the auditor to review the documents being produced to ensure that the appropriate information has been collected, recorded, and is consistent with previous documents. Verification is primarily a quality control responsibility, and should be performed by the project team. In some organizations, it is performed by the quality assurance function. If it has been performed, the auditor need only test check to make sure the quality control function is working effectively. However, if the project does not have a documentation verification procedure in place, the auditor may need to do more extensive verification.

The auditor, during the Programming and Training Phase, needs to verify three new documents and three updated documents. The verification questions to be used for each document are the following. They are not listed in any priority order.

1. User Manual verification questions
   (a) Are the functions described sufficiently?
   (b) Is the User Manual written in non-ADP terminology?
   (c) Does the manual indicate when and how it is to be used?
   (d) Does the manual serve as a reference document?
   (e) Does the manual explain how to prepare input data and parameters?
   (f) Does the manual explain how to interpret output results?
   (g) Does the manual provide a full description of the application?
   (h) Does the manual explain all of the user operating procedures?
   (i) Does the manual explain user responsibilities related to security, privacy, and internal controls?
   (j) Does the manual describe how to detect and correct errors?
   (k) Does the manual describe how to recover operations?
   (l) Does the manual describe how to perform a file query procedure?

2. Operations/Maintenance Manual verification questions
   (a) Does the manual provide computer operations personnel with a description of the software?
   (b) Does the manual provide computer operations personnel with the instructions necessary to operate the software?
   (c) Does the manual provide computer operations personnel with sections on non-routine procedures, remote operations, and security requirements?
   (d) Does the manual provide computer operations personnel with error procedures?
   (e) Does the manual provide computer operations personnel with recovery procedures?
   (f) Does the manual provide maintenance programmers with the information and source code necessary to understand the programs?
   (g) Does the manual provide the maintenance programmer with an overview of the architecture/structure of the system?
   (h) Does the manual provide the maintenance programmer with maintenance guideline procedures?
   (i) Does the manual provide the maintenance programmer with the design of internal control and security procedures so that they can be individually maintained?

3. Installation and Conversion Plan
   (a) Does the plan explain how to install the software?
   (b) Does the plan explain how to activate security procedures?
   (c) Does the plan explain how to interconnect the software with other related software packages?

(d) Does the plan explain how to install the software onto the operating environment?
(e) Are the parts of the plan directed toward staff personnel presented in non-technical language?
(f) Are the parts directed toward operations personnel presented in suitable terminology?

4. System Decision Paper
   (a) Has the System Decision Paper been reviewed and approved by the responsible participants?
   (b) Has appropriate information been incorporated into the System Decision Paper to verify the correctness of that document?
   (c) Has this document been updated to reflect changes in strategy occurring during this phase?

5. Project Plan
   (a) Is there a strategy for managing the software?
   (b) Are goals and activities stated for all phases and subphases?
   (c) Are resource estimates stated for the duration of the system development process?
   (d) Are the intermediate milestones, including management and technical reviews, stated and being met?
   (e) Are the methods for design, documentation, problem reporting, and change control given?
   (f) Are there supporting techniques and tools identified?
   (g) Has this document been updated to reflect changes in strategy occurring during this phase?
   (h) Are controls in place to determine whether or not milestones have been met?
   (i) Are appropriate actions taken if milestones are not met?

6. Validation, Verification, and Testing Plan and Specifications
   (a) Does the document include a plan for testing the software?
   (b) Does the plan include detailed specifications, descriptions, and procedures for all system tests?
   (c) Does the test plan include a test data reduction and evaluation criterion?
   (d) Is the VV&T Plan related to the system plan?
   (e) Does the system plan drive the VV&T Plan?
   (f) Does the VV&T Plan include general project background and information on the proposed solution to any mission deficiency(ies)?

(g) Does the VV&T Plan include VV&T requirements, measurement criteria, and constraints?
(h) Does the VV&T Plan include procedures to be applied during development in general and in each phase?
(i) Does the VV&T Plan include supporting information for VV&T selections made?
(j) Does this document include appendices which describe project and environmental considerations?
(k) Does the VV&T Plan include tests of security and internal controls?
(l) Does the document include appendices which define the testing technique and tool selection information?
(m) Has this document been updated to reflect changes in strategy occurring during this phase?

7. User Manual and Operations/Maintenance Manual Change Control
   (a) Is a procedure in place to keep the training materials in these manuals up-to-date?
   (b) Are there controls in place to ensure that training materials based on these manuals are updated as associated information in the manuals are updated?

4.6.3.4.2 Interview Key Participants - The auditor should interview all of the participants in the Programming and Training Phase. If there are numerous participants in any functional area, (e.g., several Sponsors) the auditor should select the most appropriate individuals to interview to ensure that they have fulfilled their proper role and responsibilities.

Listed below are the key questions that the auditor should ask of the responsible participants:

1. Information Resources Management (IRM) Official
   (a) Has the IRM Official reviewed the updated System Decision Paper?
   (b) Has the IRM Official approved the updated System Decision Paper?
   (c) Has the review of the Paper been done in consultation with a Sponsor/User and ADP Manager?

2. System Security Officer (SSO)/Internal Control Officer (ICO)
   (a) Has the SSO/ICO reviewed the SSO/ICO components of the User Manual?
   (b) Has the SSO/ICO reviewed the SSO/ICO components of the Operations/Maintenance Manual?
   (c) Has the SSO/ICO reviewed the SSO/ICO components of the Installation and Conversion Plan and the VV&T Plan and Specifications?

3. Sponsor/User
   (a) Has the Sponsor/User approved the revised Project Plan?
   (b) Has the Sponsor/User approved the revised User Manual?
   (c) Has the Sponsor/User approved the revised Operations/Maintenance Manual and Installation/Conversion Plan?
   (d) Has the Sponsor/User approved the updated System Decision Paper?
   (e) Has the Sponsor/User initiated the appropriate user training tasks?
   (f) Has the Sponsor/User approved the VV&T Plan and Specifications?

4. Project Manager(PM)/Contracting Officers Technical Representative (COTR)
   (a) Has the Project Plan been updated?
   (b) Has the VV&T Plan and Specifications been revised?
   (c) Has the Users' Manual been developed?
   (d) Has an Operations/Maintenance Manual been developed?
   (e) Has the Installation and Conversion Plan been developed?
   (f) Has it been ensured that appropriate programming was performed?

5. System Security Specialist/Internal Control Specialist
   (a) Have the SSO/ICO components of the Users' Manual been reviewed?
   (b) Have the SSO/ICO components of the Operations/Maintenance Manual been reviewed?
   (c) Have the SSO/ICO components of the Installation and Conversion Plan been reviewed?
   (d) Have the SSO/ICO components of the VV&T Plan and Specifications been reviewed?

6. Contracting Officer
   (a) If appropriate, has the contract been awarded?

7. Contract Auditor
   (a) If appropriate, has contract compliance been assured?

8. ADP Manager
   (a) Have the VV&T relevant parts of the User Manual been reviewed?
   (b) Have the VV&T relevant parts of the Operations/Maintenance Manual and Installation and Conversion Plan been reviewed?
   (c) Has the requested technical support been provided to the Project Manager?
   (d) Has the requested technical support been provided to the Sponsor/User?

9. Quality Assurance (QA) Specialist
   (a) Has the program definition been reviewed for compliance to design and data processing standards?
   (b) Has the program code been reviewed for compliance to design and data processing standards?
   (c) Has the documentation been reviewed for compliance to design and data processing standards?
   (d) Has the training been reviewed for compliance to design and data processing standards?

4.6.4 Customize Audit Objectives

The audit objectives defined for this phase may need to be customized depending upon the design methodology used, and whether or not the AIS is acquired through contract or purchase.

4.6.4.1 Design Methodology Audit Considerations - The two audit objectives for this phase need to be customized based on the following three factors:

1. Status of design up to this point - The fewer problems involved in this application, the less need for audit involvement during this phase. Generally, if design is properly done, the audit involvement during this phase need only be minimal. Any problems can be readily detected by auditors in the next phase.

2. Type of design methodology used - Audit involvement will change significantly depending on whether the software is developed in-house, contracted, or purchased.
   (a) For in-house developed software, the audit involvement should be at key management checkpoints, normally at the end of developmental phases.
   (b) For contracted software, the audit involvement must be specified in the contract. Again, it would be at key management checkpoints, but it would be those checkpoints specified in the contract. These should coincide with the contractor's developmental phases.

(c) For purchased applications, the only audit involvement would be an assessment of the design methodology for the purpose of determining whether adequate controls were incorporated to develop an effective application. This would be done in preparation for a buy/no-buy decision. In addition, it will change significantly depending on whether more traditional statement-level languages are used for development, such as COBOL, or whether fourth-generation languages such as NATURAL are utilized. Many of the fourth-generation languages are really an output of the system Design Phase, and thus there is minimal work for the implementation team during this phase.

3. Technology integration factors - During the implementation phase, the risk attributes of technology integration can be reassessed to evaluate the implementation risk. The greater the risk, the greater the need for audit involvement. The technology integration attributes that need to be considered in evaluating the scope and objectives of audit work include:
   (a) Make-up of project team in relation to technology used (number, training and experience);
   (b) Applicability of the data processing design methodologies and standards to the technology in use;
   (c) User knowledge of related technology;
   (d) Margin for error (i.e., is there reasonable time to make adjustments, corrections, or perform analyses before the transaction is completed?);
   (e) Availability of automated error detection/correction procedures;
   (f) Degree of dependence on AIS; and
   (g) Criticality of interfaces with other systems and external organizations.

4.6.4.2 Contracting/Purchase Audit Considerations - If the software is obtained through purchase and/or contract, the audit role will change. Rather than working with the project team, the auditors will be working with the COTR and the contractor personnel.

It is important in the issuance of any contract that the contract provide auditors the right to review contractor work. Without this contractual provision, the contractor may deny the auditor access to documents and/or charge additional fees for those reviews.

If off-the-shelf software is acquired, this step will collapse into a training phase. Because training is agency dependent, it will still be necessary to develop the training plan for training end users in use of the software. It is normally also necessary to develop operations manuals for purchased and/or contracted software, because of the unique internal operating conventions within an agency.

No specific changes in audit approach are required for contracted or off-the-shelf software. The specific contracting/purchasing concerns that the auditor should have are:

1. If the contractor/vendor should go out of business, would the source code ownership revert to the government?

2. Will the training material be customized for the department/agency that will use the AIS outputs?

3. If the implemented software is defective, will the vendor fix that software at no additional cost?

4. Will defects in the software be fixed on a timely basis?

5. Are provisions included in the contract that permit changes to be made to the AIS during development?

6. If the AIS/software is contracted, is there an effective communication line established between the Sponsor/User and the contractor for clarification of design specifications prior to implementation?

7. For purchased software, is there a user group, or customer base that can be used to inquire into problem and operation resolution?

4.6.5 Detailed Audit Testing

The purpose of this phase is to develop all applications and conversion programs and perform initial unit testing. Tasks to be accomplished in this phase are:

1. Flowchart solutions;
2. Code data structures;
3. Translation of program specifications into source language statements;
4. Installation of software packages and security features and establishment of communication network;
5. Performance of component and unit testing; and
6. Production of operating instructions and systems User Manuals while consulting with user and computer service organizations.

By the end of this phase, the following documentation should be finalized:

1. User Manual.
2. Operations/Maintenance Manual.
3. Installation and Conversion Plan

4.6.5.1 Introduction - During detailed audit testing, the auditor needs to evaluate the adequacy of the programming effort by reviewing test results--unit, integration, and system testing. First, the auditor should evaluate the results of Quality Assurance reviews of testing efforts. The results of this evaluation should determine the effectiveness of Quality Assurance's reviews, and thereby determine the nature and extent of audit involvement in this SDLC phase. Should there not be an effective Quality Assurance function, the auditor will need to evaluate the adequacy of testing efforts himself/herself.

In addition to evaluating testing, the auditor needs to evaluate the adequacy of documentation--user, programming, maintenance, installation, and training manuals--and training. Again, the auditor should review Quality Assurance efforts in these areas, and not duplicate the work done by that function. If, however, there is not an effective Quality Assurance function, the auditor will need to evaluate the adequacy of the documentation produced up to this point in the SDLC process. Note that in many agencies this is a weak part of this SDLC phase, and one to which the auditor can make a significant contribution since he/she needs to use this documentation to understand the system, just like any system user. In addition, the auditor should attend training sessions on the system (just like any other system user) to determine the adequacy of training efforts.

There are a number of automated tools that can be used during this and the next phase. Note that some of the tools are described in this phase for use in validating executable program code, and some are included in the final development phase. The auditor should determine if tools in one phase might be equally appropriate for accomplishing audit objectives in the other phase.

4.6.5.2 Programming and Training Phase Audit Tests - The Programming and Training Phase test program is designed to assist the auditor in evaluating this phase. The questionnaire (see Table 4.4) outlines the more common audit objectives. (Note that the customization step may change these slightly.) For each objective, the auditor will be provided with one or more tests to perform, and for each test, one or more tools and techniques will be suggested.

4.6.6 Audit Results/Reporting

The result of the Programming and Training Phase review should be documented and given to project management. It is important that deficiencies are identified, the potential effect of those deficiencies on meeting system mission described, and given to project manage-

ment on a timely basis. Delays in submitting review reports could significantly increase the cost of correcting deficiencies.

4.6.6.1 Potential Deficiencies - In the Programming and Training Phase some deficiencies occur more frequently than others. The following list of deficiencies are among the more common ones for this phase, and are provided to assist the auditor in identifying them:

1. Documents and/or tasks of this phase are not completed or are not completed on time, i.e., milestones are met but documents/tasks are not completed.
2. Milestones are not met due to incomplete tasks of this phase.
3. Applications are coded which could be done more economically through contracting or purchasing off-the-shelf software.
4. Documentation for programming and training is not prepared in accordance with standards, or not prepared at all, resulting in additional maintenance and operational costs.
5. The program documentation is not maintained in a current state, meaning that as the programs are changed the documentation is not updated. The net result is the documentation is unusable for maintaining the system.
6. No quality control is exercised over the documentation to ensure that it is complete and in compliance with standards.
7. Programs are not fully tested, resulting in defective programs being placed into operation.
8. The users of the application are inadequately trained in the use of the application, so users either misuse the software, or are unable to use software features.
9. User Manuals are not prepared, or are not prepared in accordance with standards, resulting in transactions being incorrectly entered, processed, or output being improperly utilized.
10. Audit and quality assurance tools and techniques are not included or not properly implemented in the AIS.

4.6.6.2 Potential Effects of Deficiencies on Meeting System Mission - Deficiencies in programming will result in inaccurate or incomplete processing. The result may be abnormal terminations in processing, resulting in reruns of processing and late delivery of outputs. Deficiencies not uncovered through operational controls will result in improper processing by AIS users.

Deficiencies in documentaion and training can and do result in operational malfunctions and erroneous processing. Also, deficiencies in documentation and training may result in uneconomical operations because tasks need to be performed several times in order to get them performed correctly.

The auditor probably will not be able to quantify the impact of these potential deficiencies; however, he/she should be able to demonstrate the potential adverse effects which could occur due to inadequate programming, documentation, and training. Specifically, the auditor could: 1) process test data to show that the system was not properly programmed to prevent erroneous processing; 2) compare user and programmer documentation to identify discrepancies between these two critical documents; and 3) compare user documentation to training documentation and instructions to identify inconsistencies.

4.6.7 Reassess Audit Strategy

At the end of the Programming and Training Phase, the auditor needs to determine the amount of audit involvement to be expended in the final phase. As with other phases, if there are minimal problems detected by the end of this phase, the auditor may not need to expend extensive effort in the Evaluation and Acceptance Phase. Conversely, if the auditor suspects that there are potential weaknesses in the system, extensive audit involvement may be warranted during the next phase.

The auditor should also complete any post-implementation audit programs, tools, and techniques during this phase. As the Sponsor/User is evaluating the system during the next phase, the auditor should be prepared to evaluate the audit program developed for use during operations. At a minimum, this audit program should include:

1. A list of potential areas for audit investigation;
2. Tools for file analysis and/or software packages for use during operation for file analysis;
3. Step-by-step audit programs for the audit team to use in auditing the operational AIS; and
4. A permanent working file on AIS, including key aspects of documentation, with references to official AIS documents.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	Program documentation and programming standards should be enforced to ensure that documentation is maintained in accordance with management policy.	1. Review project documents to ensure they include procedures for compliance with ADP procedures, standards and policies. 2. Review completed documents for compliance to standards and policies.	Structured interview -- Validate through project personnel how they ensure compliance to the appropriate ADP standards and policies. System development methodology review checklist -- The system development methodologies may provide checklists for use in reviewing compliance to the methodology and appropriate procedures and standards.
2.	Each program should have adequate test data prepared to validate the functioning of the executable source code.	1. Create sufficient test data to validate the important functions of the AIS.	Test data -- Process auditor-generated test data to validate the adequacy of program/system internal controls. Audit software -- Packages provide routines which will analyze data and extract from production files a representative number of records for test purposes. Program test matrix -- Prepare a matrix which tests data elements on one axis and all valid and invalid types of data on the other. Assure that all valid and invalid combinations of data have been tested. Flowcharting packages -- Create a flowchart from the source code to validate the functioning of the program.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	Each program should include a detailed narrative description of the processing to be performed and the logic of that processing. (Note that documentation may be included within the program, maintained on electronic media outside the program, or may be prepared manually.)	1. Review the detailed narrative prepared as part of the program documentation, and determine that it conforms to the original system definition narrative, and that it is adequate for understanding and maintenance purposes. 2. Determine if there is an understandable "link" between the code and the supporting requirements.	Quality control/quality assurance review -- If an independent group within data processing performs a review of this type, the auditor can evaluate the review documentation to determine whether that review can be relied upon as a test of performance for this audit objective. Software packages -- Certain software packages automatically generate the documentation needed to understand individual source programs or groups of programs, including graphic record layouts. Because documentation is in a standardized format, it only requires minimal training to understand the structure and content of that documentation. The auditor can use it to evaluate the program functionality. Peer review -- Another programmer can review a program to ensure the accuracy and completeness of the program documentation. System development methodology checklist -- The development methodology may include checklists for reviewing the adequacy of program documentation, and its consistency with system documentation. Flowcharting packages -- Create a flowchart from the source code to validate the functioning of the program.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
4.	All of the source code should be executed during testing.	1. Determine that all of the executable lines of source code have been exercised during testing.	Instrumentation -- Use a package that will count the source codes exercised during testing. The programs should include all of the functions described in the program specification.
		2. Validate that all of the functions specified for the program have been incorporated into the program.	Program test matrix -- Prepare a matrix which lists the program functions on one axis of the matrix and the program requirements on the other axis of the matrix. Then cross-reference in the matrix the implemented function to the functional specifications.
5.	Run manuals for operators' use should be prepared and adequately documented in an Operations Manual.	1. Assure that the operator manuals are in compliance with documentation standards, and that they include for each job step the following information: a) Program function b) Hardware requirements c) Explanation of all console messages together with appropriate operator response d) Output creation and its disposition e) Proper identification of output file labels f) Appropriate restart or notification procedures specified for error or failure conditions	Operator run manual checklist -- Checklists should be available in the system development methodology that indicate the contents of the operator manual. Also use the list in Section 4.6.3.4.1 as an additional checklist.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
5.	(continued)	g) Checkpoint controls for proper run-to-run control	
6.	A Maintenance Manual should be prepared with adequate information on projected maintenance needs and problems.	1. Review the Maintenance Manual for projected a) periodic software needs b) periodic hardware needs c) possible problem areas	Use information found in system development methodology for appropriate information to be found in the maintenance manual, as well as the concerns expressed in Section 4.6.3.4.1.
7.	Manuals for users should be prepared and adequately documented.	1. Verify that User Manuals exist which include the documentation specified by the ADP standards, and assure that, for each User Manual, documentation includes the following: a) Specifications and layout for input data b) Need for control totals c) Manner of submitting data d) Manner of receiving outputs e) Manner of querying the system f) Responsibility for converting data into machine-readable form g) Responsibility for resolving errors or other inaccuracies	User Manual checklist -- Checklists should be available in the system development methodology that indicate the contents of the User Manual. Also use the list in Section 4.6.3.4.1 as a checklist.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
7.	(continued)	h) Parameter for priority assignment for processing remote job entry (RJE) type work	
8.	A Training Plan should be prepared and documented in detail. This may be found within or based upon the User Manual and the Operations/Maintenance Manual.	1. Determine whether a written Training Plan has been prepared in detail.	Training Plan checklist -- System development methodology and/or ADP standards should identify what attributes should be included within the Training Plan.
		2. Confirm with user department management that the Training Plan anticipates its needs adequately.	Use structured interview -- Inquire of user management regarding the adequacy of the Training Plan.
9.	Determine that good programming practices have been employed to take advantage of modern software engineering and computer efficiencies.	1. Determine whether the AIS has been written in accordance with data processing standards and procedures.	Programs should contain checklists of standards complied with and not complied with; or programs may be reviewed by the quality assurance function to verify compliance to standards.
		2. Use software packages to analyze the efficiency of program code.	There are software packages that can be used to measure the efficiency of operation.
10.	Each program should be tested to ensure that it correctly performs the functions assigned to that unit.	1. Validate that there is at least one test condi-tion for each program function.	Examine the Test Plan to determine that each function has been defined, and that there is a test condition to evaluate that function.
		2. Ensure that during the test there has been adequate coverage of program instructions.	There are software packages that can be used to count the instructions exercised during tests to validate whether an adequate coverage of the code has been exercised during testing.

TABLE 4.4 - PROGRAMMING AND TRAINING PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
11.	An Installation and Conversion Plan should be prepared and adequately documented.	1. Verify that the Installation and Conversion Plan has been produced and, at a minimum, satisfies concerns in Section 4.6.3.4.1.	Use the list in Section 4.6.3.4.1 for the Installation and Conversion Plan as a checklist.
12.	An updated System Decision Paper should have been produced at the start of this phase.	1. Verify that an updated System Decision Paper has been produced and is backed up by new information developed at the end of the last phase.	Review the document. Use structured interview of responsible participants.
13.	A change control process should be in place for the User Manual and the Operations/Maintenance Manual.	1. Verify that a change control process has been defined and is implemented in terms of timing criteria and responsible personnel.	Use structured interview to confirm that such a change control process is in place.

4.7 AUDIT PARTICIPATION IN THE EVALUATION AND ACCEPTANCE PHASE - PHASE V

The objective of this phase is to ensure that the AIS is acceptable to the users prior to placing the system into a production mode. During this phase, unit testing will be completed, and integration and system testing undertaken. The results of these tests will provide user management with the information necessary to make a decision on acceptance, modification, or rejection of the AIS. The audit objective in this phase is to ensure that the total system and data are validated and fully meet all user requirements. The auditor should continue to emphasize internal control requirements as an area requiring specific audit attention. The fulfillment of this objective may be done in conjunction with the VV&T Plan, or it may be independent of that plan.

4.7.1 Primary Audit Objective of the Evaluation and Acceptance Phase

The primary audit objective of this phase is to:

"Ensure that the total system and data are validated as fully meeting all user and internal control related requirements."

The fulfillment of this objective should be accomplished by reviewing the work of the VV&T test team, and conducting additional tests as appropriate. The actual performance of the task is normally too time-consuming for audit to perform. It has been estimated that this phase of the developmental process can consume up to 30 percent of the developmental effort.

If testing is properly performed, a test plan, test results, and a test report will be available. [Note that many Federal agencies neither plan nor formalize the results of testing into a report.] The test plan should indicate the AIS functions, and then cross-reference them to the tests designed to validate the correct operation of those functions. Test results should be specifically documented and retained. The test report should indicate the results of those tests, and then relate the test results back to the function, indicating whether or not it performs correctly.

If the test results and AIS Life Cycle Matrix are completed and prepared for the test report, the auditor's role becomes significantly easier. In these instances, the auditor only needs to perform sufficient tests to ensure himself/herself that the test results are correct. The auditor should then be able to draw the same conclusions from the test results and AIS Life Cycle Matrix as the test team.

In completing the audit objective, the auditor should perform the same six steps described in the other development phases. These steps are individually described below for this phase.

4.7.2 Overview of the Evaluation and Acceptance Phase

The evaluation of the AIS should be conducted in accordance with the revised VV&T Plan. Completed code will undergo testing, as described in the revised VV&T Plan. Generally, three types of program testing are performed: unit, integration, and system. If performed properly, unit testing will then validate the functioning of the unit; integration testing will validate the interfaces between the units and the operating environment; and system testing will validate the interaction between the application system and the user area. It is recommended, but often difficult to achieve, that unit testing be completed before integration testing commences, and integration testing be completed before system testing commences.

It is important that adequate time be allocated to testing. Previous GAO reports have indicated that software testing is basically an underplanned and undermanaged part of the developmental process. This occurs because frequently the previous phases are completed late, even though the installation date remains fixed. In order to meet the installation deadline, the amount of time and effort allocated to testing deteriorates to the point that it is ineffective in accomplishing its objective.

After the review, analysis, and testing of the system, including execution of the programs on test data, the AIS should be field tested in one or more representative operational sites. For particularly sensitive AISs, disaster recovery and continuity of operations plans should be fully documented and operationally tested as well. Using actual transaction data, if designated a "sensitive" system, it should be certified for technical adequacy in meeting its security requirements by an appropriate authority, prior to accreditation and installation. Before certification, all VV&T test results should be documented and a comparison of actual and expected results made.

The OMB Circular A-130 and FIPS PUB 102 security evaluation should be part of the broader test results/test evaluation report. The accreditation statement, the last key activity of the phase, would be a statement from the responsible accrediting official (e.g., Sponsor or IRM Official) that the system is operating effectively and is ready to be installed. Any caveats or restrictions should be provided at this time.

4.7.2.1 Participants and Their Tasks - All or most of the participants responsible for the AIS play an active role in evaluation and acceptance. In the early phases, the responsible participants are frequently senior people in the area of involvement. For example, the manager or

assistant managers of the user area may be personally involved in the early developmental phases. As the work gets more technical, the responsibilities are frequently delegated downward to lower-level people in the operational areas. During the Evaluation and Accep-

tance Phase, as critical decisions have to be made, the more senior people should again be involved.

The responsibilities of the participants in the Evaluation and Acceptance Phase are:

1. Information Resources Management (IRM) Official - Approves updated System Decision Paper to advance to Phase V, in consultation with Sponsor/User and ADP Manager (occurs between phases).

2. System Security Officer (SSO)/Internal Control Officer (ICO) - Reviews Test Results and Evaluation Report and SSO/ICO components of Installation and Conversion Plan.

3. Auditor(OIG) - Reviews/evaluates revised Project Plan, revised Installation and Conversion Plan, and Test Analysis and Security Evaluation Report; updates Audit Program.

4. Sponsor/User - Approves revised Project Plan and Installation and Conversion Plan; updates System Decision Paper; oversees training; accepts (accredits) system for operation.

5. Project Manager/Contracting Officer's Technical Representative (COTR) - Updates Project Plan; supports and oversees Test Analysis and Security Evaluation Report and certifies system security; revises User Manual, Operations/ Maintenance Manual, and Installation and Conversion Plan based on test results.

6. System Security Specialist/Internal Control Specialist - Reviews Test Analysis and Security Evaluation Report and SSO/ICO impacted documentation updates to User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan.

7. Contracting Officer - If appropriate, awards contract.

8. Contract Auditor - If appropriate, assures contract compliance.

9. ADP Manager - Directs test reviews and validated VV&T components of Installation and Conversion Plan; continues to provide technical support.

10. Quality Assurance (QA) Specialist - Reviews VV&T results and advises responsible participants on system achievement of Needs Statement.

4.7.2.2 Evaluation and Acceptance Phase Document - The auditor will evaluate the work performed in this phase by looking at the phase documentation. The phase produces one new document, and three updated documents (System Decision Paper, Project Plan, Installation and Conversion Plan). The new document is:

1. Test Analysis and Security Evaluation Report (NBS SP 500-98, DOD-STD-7935 "Test Analysis Report," OMB A-130, OMB A-123, FIPS PUB 102) The purpose of the Test Analysis and Security Evaluation Report is to (1) document the test analysis results and findings; (2) present the demonstrated capabilities and deficiencies, including the Security Evaluation Report needed for certification of the AIS; and (3) provide a basis for preparing a statement of AIS/software readiness for implementation.

4.7.3 Audit Survey

The main source of information for this phase will be the audit results and workpapers from previous phases. If the same individuals are involved in evaluation and acceptance, as were involved in previous phases, background preparation work should be minimal. However, the auditor is still concerned with the flow of work, the assurance that the responsible participants fulfilled their roles, and acquiring and reviewing the documentation produced during this phase.

4.7.3.1 Review Programming and Training Phase Outputs - At this point, the AIS has been completed. The objective of this phase is to identify and remove defects from the AIS. This is accomplished through creation of a series of test conditions, which, when processed against the executable code, produce the proper results by which the system will be judged correct (or inadequate).

The auditor may wish to review some of the documents from the earlier phases because they indicate what the system is supposed to do. The programming phase documents are oriented toward what the system does to meet its objectives while the User Manual and Training Manual explain how the system is to be operated by the end users. It is recommended that the auditor understand both the what and the how, in preparation for reviewing this final phase of the system development process.

It is also important that the auditor ensure that the test data and testing documentation is saved for use in validating subsequent changes to the AIS and for auditor usage as required.

4.7.3.2 Review Evaluation and Acceptance Phase Plans - The final phase is one which is frequently squeezed between the point where the programs are complete, and the date when those programs must be placed into production. If the production date is firm, insufficient time

may be allocated to this phase. Therefore, it becomes essential that the auditor determine that at least the most critical AIS functions are tested.

It is unrealistic to expect exhaustive testing to occur, though it is certainly desirable. There will always be compromises between budget and schedule, and complete testing. In many instances there are no options regarding when the AIS is placed into production, particularly when it is mandated by legislation. What is important is to optimize the test time available.

4.7.3.3 Gather Information on Evaluation and Acceptance Phase Status - Reports should be maintained on the status of testing. The criteria for testing should be included in the VV&T Plan. This will indicate which functions are to be tested, and what conditions will be used to test those functions.

In the hierarchy of testing, the units or programs should be tested first. Once these have been validated as performing correctly, the integration or interfaces between the units or programs are tested. Once those interfaces have been validated, the acceptance test occurs, which validates the interfaces between people and the system.

The status reports on testing should indicate which functions have been tested, which functions work, which functions are in the process of being corrected, and when those functions should be retested. The auditor, at any point, should be able to determine how many functions have been validated and how many remain unvalidated. If this status information is not available, the auditor should be concerned over whether the end product of testing will adequately indicate AIS performance prior to the system being placed into production. Without this type of information, management cannot make a knowledgeable decision regarding installation and operation of the AIS.

During this phase, the auditor should obtain for analysis purposes the following documents:

1. Test Analysis and Security Evaluation Report, including certification and accreditation statements.
2. Updated Installation and Conversion Plan.
3. Updated User Manual.
4. Updated Operations/Maintenance Manual (including change control).
5. Updated Project Plan.

4.7.3.4 Verify Information on the Evaluation and Acceptance Phase Status - By the time this phase commences, all of the work necessary to develop the AIS should be complete. The organization should have an executable AIS. What is needed is to be assured that the executable system meets the system requirements/specifications.

4.7.3.4.1 Review Documents - The flow of work in the Evaluation and Acceptance Phase is primarily a flow of testing. This flow is illustrated in Figure 5. The flow shows that there are many modules (i.e., computer sub-programs) developed during this phase. Each of those modules needs to be individually tested. The modules are then pulled together into programs. Note that some of the programs may involve utility programs and other aspects of operating software. These programs are then tested to validate that the multiple modules work correctly when intercoupled. Lastly, the programs are all put together as an AIS, and that AIS is validated to ensure that it works in the operating environment, that it works when interfacing with other systems, and that it meets user requirements.

The auditor must become familiar with the flow of work during this phase. This includes familiarization with the various types of testing and the expectation from those tests. As in other aspects of system development, the exact flow of documents will vary from methodology to methodology, and within agencies using the same methodology.

The Evaluation and Acceptance Phase produces one new document (Test Analysis and Security Evaluation Report), and five updated documents (Audit Plan, Project Plan, User Manual, Operations/ Maintenance Manual, Installation and Conversion Plan). The auditor should look at all of these documents, but put emphasis on verifying that the Test Analysis and Security Evaluation Report properly implements and accomplishes the test plan objective, and that the test results are properly reflected in the Security Evaluation Report.

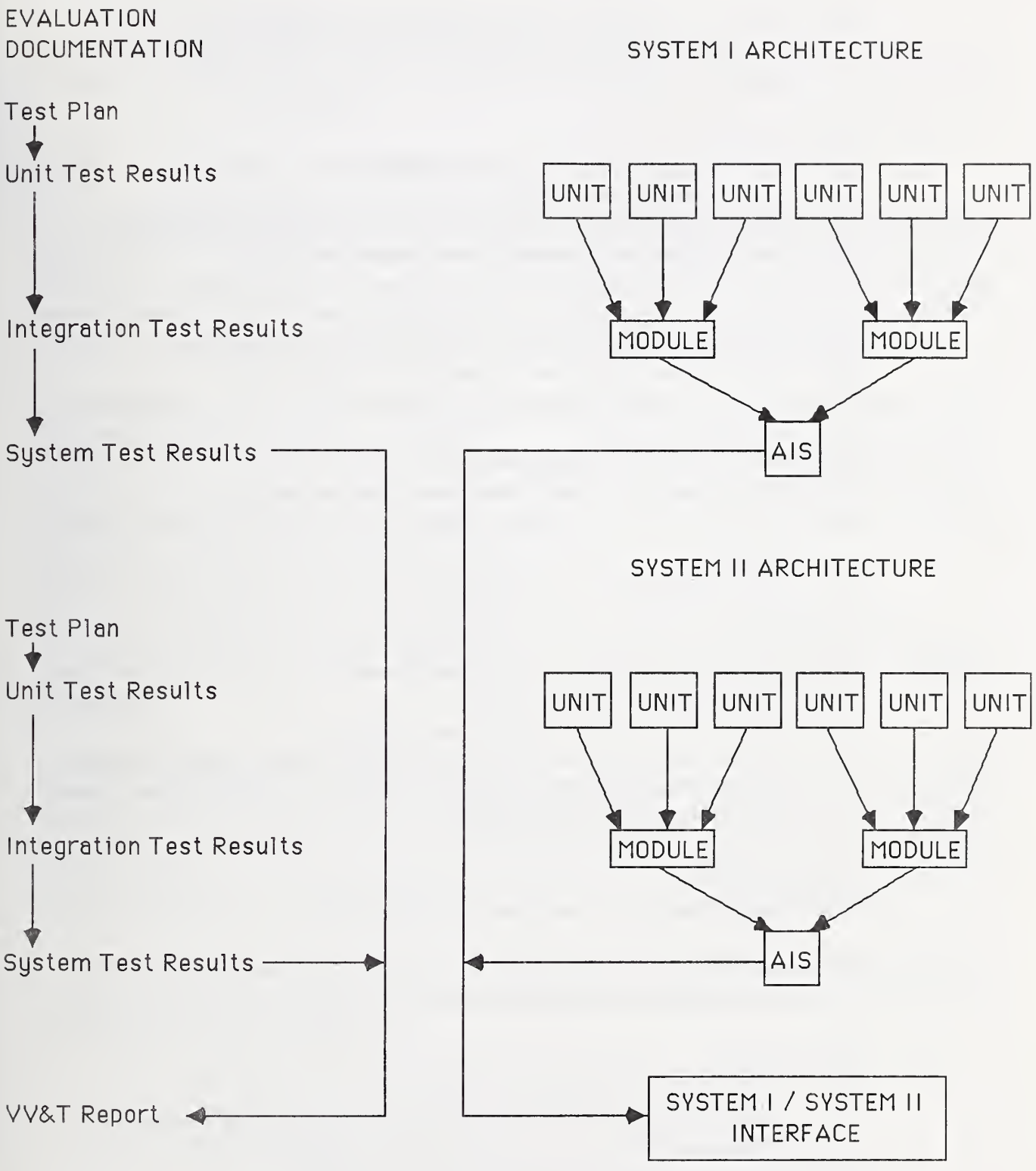
4.7.3.4.2 Interview Key Participants - The auditor needs to verify that all of the appropriate responsible participants are involved in this phase, that they have been assigned the appropriate role, and that they have correctly fulfilled that role. This step is normally done by interviewing the involved participants to verify their needed participation.

Listed below for each of the desirable participants are the questions that the auditor needs to ask those participants:

1. Information Resources Management (IRM) Official
   (a) Have you approved the updated System Decision Paper?
   (b) Did you review that paper in consultation with the Sponsor/User and ADP Manager prior to approval?

2. System Security Officer (SSO)/Internal Control Officer (ICO)
   (a) Have you reviewed the test results?

Figure 5. FLOW OF EVALUATION WORK



(b) Have you reviewed the Security Evaluation Report?
(c) Have the SSO/ICO components of the Installation and Conversion Plan been reviewed?

3. Sponsor/User
   (a) Did you approve the revised Project Plan?
   (b) Did you approve the revised Installation and Conversion Plan?
   (c) Did you make the necessary updates in the System Decision Paper?
   (d) Have you/your area overseen the necessary training?
   (e) Did you as Sponsor/User accept the system for operation?

4. Project Manager/Contracting Officer's Technical Representative
   (a) Did you make appropriate updates to the Project Plan?
   (b) Did you support and oversee the Test Analysis and Security Evaluation Report?
   (c) Did you certify the system security?
   (d) Did you revise the User Manual, based on test results?
   (e) Did you update the Operations/Maintenance Manual, based on test results?
   (f) Did you update the Installation and Conversion Plan, based on test results?

5. System Security Specialist/Internal Control Specialist
   (a) Did you review the test results?
   (b) Did you review the Security Evaluation Report?
   (c) Did you ensure that the updates to the User Manual, Operations/Maintenance Manual, and Installation and Conversion Plan reflect any impact on the SSO/ICO documentation?

6. Contracting Officer
   (a) If appropriate, have you awarded the contract?

7. Contract Auditor
   (a) If appropriate, have you assured contract compliance?

8. ADP Manager
   (a) Did you direct testing?
   (b) Did you review the validated VV&T components of the Installation and Conversion Plan?
   (c) Did you provide the requested technical support?

9. Quality Assurance Specialist
   (a) Did you review the VV&T test results?
   (b) Did you advise responsible participants on system achievement of Needs Statement?

4.7.4 Customize Audit Objectives

The specific audit objectives to be accomplished during this phase will vary depending on management's need. If the project team does not have an adequate test plan, management may ask the auditors to play a more active role in testing. Sometimes the auditors perform some of the testing that occurs during this phase. While this is not recommended, it is sometimes a necessity because testing would not otherwise be performed.

The test program outlined for this phase includes the more common audit objectives for this phase. It is those objectives that need to be customized based on the needs of management, as well as the audit evaluation of previous phases. This phase is the auditor's last opportunity to evaluate the system prior to its being placed into production. The greater the risks associated with the system, or the greater the concerns uncovered in previous phases, the greater the need for audit involvement during this phase.

4.7.4.1 Evaluation and Acceptance Phase Methodology Audit Considerations - Development activities are frequently deficient with respect to testing. They may include some test documents but are usually not extensive. Some methodologies contain no test strategies/-documents.

Development methodologies were developed years before test methodologies were developed. FIPS PUB 101 on VV&T [FIPS101], GAO's [GAO81-3] "Evaluating Internal Controls in Computer Based Systems", and IEEE's "Standard for Software Test Documentation" [IEEE83] and "Standard for Software Unit Testing" [IEEE86] provide such a test methodology. The auditor may also want to refer to AUERBACH's "A Standard for Computer Applications" [AUER86+] and NBS SP 500-136 on software acceptance testing [NBS136].

If the development methodology is deficient in the testing area, the auditor may wish to suggest one of the above references as a test strategy. The key aspects of testing that need to be addressed during this phase are:

1. Development of an adequate test plan;

2. Execution of the test plan; and

3. Analysis and reporting of test results.

The auditor should be particularly concerned with the test report. This report should indicate not only what works and doesn't work, but have an opinion from the test group regarding the adequacy of the system to be placed into a production status.

Test approaches that are used by corporations include:

1. An independent test team (i.e., a group of people independent of the project people, who are professional testers).

2. Users of the AIS create their own test conditions, and determine whether the AIS is acceptable to them for use in production.

4.7.4.2 Contracting/Purchase Audit Considerations - The Evaluation and Acceptance Phase does not change significantly whether the software is developed in-house, through contract, or off-the-shelf purchase. Obviously, with contracted and off-the-shelf software there would be minimal unit testing and integration testing, with the concentration being on system testing. However, the phase is the culmination of the test plan, which in itself is customized slightly depending on the source of the software.

Contracted software introduces no particular changes in audit activity. Contractors may participate in all activities not otherwise precluded by Federal statute or departmental policy. Contractors should not be involved in performing VV&T of systems they develop due to conflict of interest issues.

Purchase of off-the-shelf software results in the following changes for project participants:

(a) Sponsor/User reviews results of all pre-award test procedures. Concurs in any customizing and award.

(b) Project Manager oversees completion of "live test demonstration" and other pre-award test procedures, and defines/approves required customizing. (If customizing is required, that process should be done by returning to a sub-process identical, if abbreviated, to that for full systems development (Phase II-IV). The Project Manager also approves award to selected bidder/offeror.

(c) ADP Manager provides technical assistance in evaluating "live test demonstration" and other pre-award test procedures. Also oversees installation of software at the test site.

Some of the specific contracting/purchasing considerations for this phase are:

1. Does the contractor/vendor have a test plan, and is it available for examination?

2. Can the contractor/vendor indicate which functions work and which functions do not work?

3. Does the contractor/vendor guarantee the specified functions to work, and if not, agree to fix them at no additional cost to the government?

4. Are the test conditions and results available to the government to validate that the system performs as specified?

5. Does the government have the right to validate the functioning of the system before accepting the system?

4.7.5 Detailed Audit Testing

The Sponsor/User will rely upon the Security Evaluation Report to determine whether or not to accept the AIS. However, the Sponsor/User is usually not technically oriented, and thus does not have the necessary background to challenge the information included within the Security Evaluation Report. The independent opinion of the adequacy of that report, provided by the auditor, can be important in determining whether or not the application will be accepted, or if it is accepted, whether any counter strategies are needed to be put into place to compensate for potential weaknesses.

4.7.5.1 Introduction - Testing is a very critical phase of the SDLC. Programs and applications must pass system and acceptance tests prior to certification for implementation. These tests cover two different areas of concern, yet they have the same goal. The system test will provide an internal assessment of the correctness, performance, and reliability of the operational system, while the acceptance test will determine user reaction to the product, its performance, installation procedure, documentation, and reliability. Once these tests have been performed, the project team will review the results to ensure the system meets user requirements and is acceptable to the user.

The auditor has two major roles in this phase of the SDLC: (1) to ensure testing is adequately planned and performed in compliance with approved standards; and (2) to ensure test results are properly evaluated and included in system documentation.

4.7.5.2 Evaluation and Acceptance Phase Audit Tests - An Evaluation and Acceptance Phase audit program is provided to assist in completing this step (see Table 4.5). The audit program includes sub-objectives for audit, suggested tests for the auditor to undertake to accomplish those objectives, and then tools that might prove helpful in conducting those tests. These are provided as guides to auditors to help them be more effective in reviewing AISs in the Evaluation and Acceptance Phase.

4.7.6 Audit Results/Reporting

Once the auditor identifies a weakness, management will need recommendations to overcome that weakness. The recommendations should be consistent with the magnitude of the variance. Variance with a minor impact may not warrant highlighting in an audit report or offering recommendations. Recommendations should be limited to those findings having a significant impact on the agency/organization mission.

4.7.6.1 Potential Deficiencies - Deficiencies identified in this phase will normally represent operational deficiencies. If they are not corrected prior to the application being placed into production, they may cause or contribute to a system failure. At this point in the development cycle there is no time to compensate for deficiencies in future phases.

Listed below are some of the more common deficiencies found in the Evaluation and Acceptance Phase. These deficiencies are listed to help the auditor ensure that one or more of the more common Evaluation and Acceptance Phase deficiencies has not been overlooked.

1. Testing does not include all of the tests included in the test plan, resulting in untested functions being placed into production.

2. A test report is not prepared, or if prepared does not adequately indicate which areas have been validated to function correctly, and which have not been validated. This results in applications being placed into production without the user knowing what works and what does not work.

3. User management is not involved in the decision whether or not to put the system into production, resulting in systems being placed in production which may have defects which, if known, would result in the user stopping the system from being placed into production.

4. The test plan, test results, and test reports are either not complete, or not prepared in a manner that can be used as ongoing maintenance documentation. This results in maintenance personnel having the costly task of reproducing test conditions and test results.

5. A parallel test is not conducted, resulting in the user being uncertain if the new system can produce the same results as the old system (applicable only when current automated capabilities are in existence).

6. The AIS is not field tested at selected locations and, therefore, does not work properly in the operational environment.

7. System development documentation is not updated to reflect the changes and activities that occurred during development. This results in maintenance occurring with inadequate documentation and with the potential of increasing the defect rate and/or costs of maintenance.

8. A written Conversion Plan is not prepared and followed, resulting in the potential for increased conversion costs and inaccurately or incompletely performed conversion tasks.

9. System security is not certified. This results in potential security vulnerabilities in the operational AIS.

4.7.6.2 Potential Effects of Deficiencies on Meeting System Mission - The impact of deficiencies in this phase should be calculated as operational defects. The auditor should identify the potential deficiency event, estimate the number of times that event will occur within the next year, determine the expected loss per event, and then multiply the two variables together to calculate the annual loss expectation. FIPS PUB 65 explains how to perform this calculation.

4.7.7 Reassess Audit Results/Plans

The auditor should conclude the audit program once the system becomes operational. The insight gained during the developmental process should be passed on to the audit team reviewing the operational system in order to properly focus and maximize audit effort. The types of insight to be included in the program was described in the previous phase.

The auditor should select the final operational audit tools during this phase. These tools should be tested (at the same time the AIS is tested) to ensure they work. Thus, the auditor undergoes an evaluation and acceptance of audit tools at the same time that user management undergoes an evaluation and acceptance of the AIS.

TABLE 4.5 - EVALUATION AND ACCEPTANCE PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
1.	Unit, module, and integration testing should be conducted according to the Test Plan and applicable ADP test standards.	1. Validate that the tests conducted are the tests included in the updated VV&T Plan.	Test Plan/Test Checklist -- The tests indicated in the Test Plan should be traced to the actual tests conducted to validate that the planned tests have been performed. Test standards checklist -- Checklists included in the system development methodology and/or developed by the ADP standards group should be used to validate that testing was performed in conjunction with the standards.
2.	Test results should be evaluated by data processing management and by user department management to determine that the system functions properly.	1. Review test documentation and verify that predetermined results were developed in advance, were compared with test results, and the two were in agreement.	Batch systems -- Playback file: several software packages provide a playback capability. The playback enables the expected results to be recorded and then compared against actual results. Comparison packages -- A number of software packages permit comparison of expected results against actual results. For on-line systems -- In on-line systems, a driver package is needed to simulate on-line processing for test purposes. Few on-line drivers are yet available, but there are some available.
		2. Validate that user management evaluated the test results. 3. Determine that OMB Circular A-130 requirement for certification of controls has been met.	Structured interview -- The auditor needs to interview user personnel to ensure they have performed the steps necessary to validate the correctness of test results.

TABLE 4.5 - EVALUATION AND ACCEPTANCE PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
3.	Test results should be recorded and retained as part of the system documentation.	1. Examine all documentation related to the testing process and assess its completeness; then verify that responsibility for retaining and updating documentation relating to system testing has been properly assigned.	Test documentation checklist -- System development methodologies may include a checklist defining the types of test documentation needed, and validating that those documents are included in the ongoing system documentation.
4.	Circumstances under which a parallel run of both existing and new systems is considered desirable should be identified, and criteria for its termination should be stated.	1. Determine whether user department management's decision to require a parallel run before acceptance test is cost/benefit justified, and if so that it was performed in accordance with criteria established in advance.	Test results comparison -- A variety of software packages will compare the results of two parallel runs, without losing the ability to compare when one or two unequal conditions occur.
5.	An updated Conversion Plan should be prepared to include assignment of individual responsibilities.	1. Ascertain that both the user department and the data processing department have reviewed and approved the updated Conversion Plan; and that the Conversion Plan is documented.	Conversion Plan checklist -- System design methodologies include checklists of the attributes that are to be included in Conversion Plans. Auditors can use this to validate the existence of the appropriate attributes of a Conversion Plan. Auditor should evaluate the accuracy of conversion of programs and data, using generalized audit software to validate correctness of conversion.
6.	Ensure that adequate provisions have been made to assure continuity of processing.	1. Verify that the following tests have been done: a) Backup and recovery b) Capacity/stress test	Use GAO "Black Book"[GAO81-3] and AUERBACH Auditing Computer Applications [AUER86+] for appropriate checklists.

TABLE 4.5 - EVALUATION AND ACCEPTANCE PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
6.	(continued)	c) Planned failure tests d) Contingency plan tests	
7.	Determine that a security evaluation, a certification, and an accreditation have been performed and appropriate documents and statements prepared.	1. Examine the security certification and accreditation statements.	Use guidelines from NBS FIPS PUB 102 and NBS SP 500-133 on security evaluation, certification, and accreditation.
8.	Determine that the Installation and Conversion Plan has been updated and currently represents the current status of the AIS.	1. Verify that the Installation and Conversion Plan contains all the necessary attributes, and that those attributes are accurate and current.	Use the Installation and Conversion Plan document checklist from the phase in which this document was prepared, and then verify the information in the User Manual against the appropriate evaluation and acceptance documentation to validate the accuracy and currency of this document.
9.	Determine that the User Manual has been updated and currently represents the current status of the AIS.	1. Verify that the User Manual contains all the necessary attributes, and that those attributes are accurate and current.	Use the User Manual document checklist from the phase in which this document was prepared, and then verify the information in the User Manual against the appropriate evaluation and acceptance documentation to validate the accuracy and currency of this document.
10.	Determine that the Operations/Maintenance Manual has been updated and currently represents the current status of the AIS.	1. Verify that the Operations/Maintenance Manual contains all the necessary attributes, and that those attributes are accurate and current.	Use the Operations/Maintenance Manual checklist from the phase in which this document was prepared, and then verify the information in the Operations/Maintenance Manual against the appropriate evaluation and acceptance documentation to validate the accuracy and currency of this document.

TABLE 4.5 - EVALUATION AND ACCEPTANCE PHASE AUDIT TESTS

#	AUDIT OBJECTIVES/ INDICATOR	AUDIT TEST	TOOLS AND TECHNIQUES
11.	Determine that the Project Plan has been updated and represents the current status of the AIS.	1. Verify that the Project Plan contains all the necessary attributes, and that those attributes are accurate and current.	Use the Project Plan document checklist from the phase in which this document was prepared, and then verify the information in the Project Plan against the appropriate evaluation and acceptance documentation to validate the accuracy and currency of this document.
12.	Determine that the System Decision Paper has been updated and represents the current status of the AIS.	1. Verify that the System Decision Paper contains all the necessary attributes, and that those attributes are accurate and current.	Use the System Decision Paper checklist from the phase in which this document was prepared, and verify the information in the Systems Decision Paper against the appropriate evaluation and acceptance documentation to validate the accuracy and currency of this document.

APPENDIX A
PCIE WORK GROUP ON
EDP SYSTEMS REVIEW AND SECURITY

A.1 SUMMARY OF BACKGROUND AND CHARGE

President Reagan established the President's Council on Integrity and Efficiency (PCIE) in March 1981 to coordinate government-wide efforts to attack fraud and waste and help ensure system integrity in government programs and operations. Chaired by the Deputy Director of the Office of Management and Budget, the Council is composed of the Inspectors General (IGs), as well as representatives from the Federal Bureau of Investigations, the Department of Justice, and the Office of Personnel Management. Among its other functions, the PCIE is charged with developing interagency programs and projects to deal efficiently and effectively with those problems concerning fraud and waste which exceed the capability or jurisdiction of an individual agency.

In October 1983, the Council decided that Electronic Data Processing (EDP) Systems Review and Security was an issue requiring formal review, and established a working group. Responsibility for the PCIE Work Group was given to the Inspector General of the Department of Health and Human Services, to be included under their ongoing Computer Security Project. Composed of OIG and management representatives from fourteen Federal departments and agencies, the group was charged with facilitating and improving Office of Inspector General/Audit organization reviews of automated information systems (AISs), particularly those systems under development. The objective of the PCIE Work Group was to improve the likelihood that auditable and properly controlled systems are being developed.

To achieve this objective, the PCIE Work Group participants drew from the Department of Defense life-cycle approach to the management of automated systems, and the National Bureau of Standards' Institute for Computer Science and Technology's (NBS/ICST's) Special Publications and Federal Information Processing Standards, to develop a system life cycle matrix for AISs. That matrix, structured around critical AIS documentation requirements is intended to clarify the role of the internal auditor vis-a-vis other key participants in the EDP planning, design, implementation, and review processes. With the audit role clearly delineated, this audit guide has been developed to facilitate the successful fulfillment of that role, focusing on systems under development and major modifications to existing systems.

A.2 WORK GROUP DOCUMENTATION ACTIVITIES

The PCIE Work Group pursued a number of activities that enabled the group to arrive at some consensus position regarding documentation needs during the SDLC. The following is a brief enumeration of those activities:

1. PCIE Work Group participants were asked to review what documentation their agencies used and to provide copies of the standards or policy to the Work Group;

2. Experienced systems staff, managers, and PCIE members met to reconcile how the documents related to one another, and each life cycle phase;

3. Selected non-Federal organizations/firms were contacted to review the approach being taken regarding their systems development/review activities;

4. National Bureau of Standards (NBS) representatives were brought in to facilitate the consolidation of NBS standards and legal requirements, with the PCIE observations and recommendations.

5. General Services Administration (GSA) representatives were contacted to support the evolution of GSA's software engineering and information resources management (IRM) procurement programs, in consonance with both NBS standards and the work group recommendations;

6. General Accounting Office (GAO) representatives were contacted to see that they generally agreed with the Work Group's view of the system development life cycle, documentation needs, and EDP review activities.

7. The Office of Management and Budget (OMB) representatives were contacted to see that the Work Group's view did not violate or disagree with the then developing revision to OMB Circular A-71 TM1, found in the subsequent OMB Circular A-130.

8. All Federal agencies were provided copies of the PCIE recommendations, and offered an opportunity to comment both on the substance of the matrix, the documents, and the direction being taken.

A.3 PCIE WORK GROUP MEMBERS

Bonnie Fisher (Project Leader)	Health and Human Services Office of Inspector General
Gail Shelton	Health and Human Services Office of Inspector General
Jim Cox	Health and Human Services Office of Inspector General
Wallace Keene	Health and Human Services Office of the Assistant Secretary for Management and Budget
Bob Gignilliat	Health and Human Services Office of the Assistant Secretary for Management and Budget
David Decker	Housing and Urban Development Office of Inspector General
Mike Houston	Department of Defense Office of Inspector General
John Lainhart	Department of Transportation Office of Inspector General
Mac MacDonald	Veteran's Administration Office of Inspector General
Roger Sies	Department of Labor Office of Inspector General
William Lee	Department of Commerce Office of Inspector General
Allen Winokur	Department of Defense Naval Audit Service
Zella Ruthberg	National Bureau of Standards Institute for Computer Sciences and Technology

Jim Hollohan	Smithsonian Institution Audit Agency
David Petrocci	Department of Treasury Office of Inspector General
Mary Ann Todd	Department of Treasury Financial Management Services
Mark Gillen	Department of Treasury IRS Internal Audit
Barry Snyder	General Accounting Office IMTEC
Jack Landers	General Services Administration OIRM
John Bjork	Small Business Administration Office of Inspector General
Larry Martin	Department of Energy Office of ADP Management
Benson Simon	Environmental Protection Agency Office of the Comptroller
Doug Hunt	National Aeronautics & Space Administration Office of Inspector General
Tyrone Taylor	National Aeronautics & Space Administration Office of Inspector General

APPENDIX B
LAWS AND REGULATIONS

B.1 SPECIFY AUDIT INVOLVEMENT

B.1.1 Standards for Audit of Governmental Organizations, Programs, Activities, and Functions(Yellow Book), GAO, 1981 Revision [GAO81-1]: In 1981, the Comptroller General of the United States (head of GAO) issued audit standards that were intended for application to audits of all government organizations, programs, activities, and functions--whether they are performed by auditors employed by Federal, State, or local governments. The standards are designed to be general in nature and apply to audits of all types. These standards are periodically updated to reflect the current GAO audit direction.

The current standards contain an optional standard regarding audit participation in systems development. The GAO strongly recommends that auditors be actively involved in reviewing the design and development of new data processing systems or applications, and significant modifications thereto, as a normal part of the audit function.

B.1.2 The Inspector General Act of 1978(PL95-452, October 12, 1978) [IGA78]: The Act established the Office of Inspector General within major Federal agencies in order to form independent and objective units:

- To conduct and supervise audits and investigations relating to programs and operations of the Department of Agriculture, the Department of Commerce, the Department of Housing and Urban Development, the Department of the Interior, the Department of Labor, the Department of Transportation, the Community Services Administration, the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration, the Small Business Administration, and the Veterans' Administration;

- To provide leadership and coordination, and recommend policies for activities designed (a) to promote economy, efficiency, and effectiveness in the administration of, and (b) to prevent and detect fraud and abuse in, such programs and operations;

- To provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action; and

- To comply with standards established by the Comptroller General (GAO) for audits of Federal establishments.

B.1.3 Budget and Accounting Procedures Act of 1950(PL81-784, September 12, 1950) [BAPA50]: Part II of this Act is cited as the "Accounting and Auditing Act of 1950". This part states that: The accounting of the Government is to provide full disclosure of the results of financial operations, adequate financial information needed in the management of operations and formulation and execution of the Budget, and effective control over income, expenditures, funds, property, and other assets.

The auditing for the Government, conducted by the Comptroller General of the United States as an agent of the Congress, is to be directed at:

- determining the extent to which accounting and related financial reporting fulfill the purposes specified;
- financial transactions have been consummated in accordance with laws, regulations, or other legal requirements; and
- adequate internal financial control over operations is exercised, and afford an effective basis for the settlement of accounts of accountable officers.

Emphasis is to be placed on effecting orderly improvements resulting in simplified and more effective accounting, financial reporting, budgeting, and auditing requirements and procedures, and on the elimination of those which involve duplication or which do not serve a purpose commensurate with the costs involved. Financial transactions of each executive, legislative, and judicial agency are to be audited by the General Accounting Office (GAO) in accordance with such principles and procedures, and under such rules and regulations as may be prescribed by the Comptroller General of the United States. In the determination of vouchers and other documents, the Comptroller General is to give due regard to generally accepted principles of auditing, including consideration of the effectiveness of accounting organizations and systems, audit and control, and related administrative practices of the respective agencies.

B.1.4 Quality Standards for Federal Offices of Inspector General, by President's Council on Integrity and Efficiency (PCIE), 1986 [PCIE86]: This document contains quality standards for the management, operation, and conduct of the Federal Offices of Inspector General (OIG). They have been formulated and adopted as advisory standards by those Inspectors General who are members of the PCIE. The subjects of the thirteen standards are:

- Maintaining Independence
- Planning
- Organizing
- Assuring Staff Qualifications

- Directing and Controlling
- Coordinating
- Reporting
- Preserving Confidentiality
- Maintaining Quality Assurance
- Reviewing Legislation and Regulations
- Receiving, Controlling, and Screening Allegations
- Investigating
- Auditing

B.2 SPECIFY INTERNAL CONTROLS

B.2.1 Federal Managers' Financial Integrity Act(PL97-255, September 8, 1982) [FMFIA82]: This Act requires internal control systems that are reasonable, to ensure that the following objectives are achieved:

- Obligations and costs comply with applicable law.

- All assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

- Revenues and expenditures applicable to agency operations are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and accountability of the assets may be maintained.

The Act directs the heads of executive agencies to:

- Make an annual evaluation of their internal controls using guidelines established by the Office of Management and Budget (OMB).

- Provide annual reports to the President and Congress that state whether agency systems of internal control comply with the objectives of internal controls set forth in the Act and with the standards prescribed by the Comptroller General. Where systems do not comply, agency reports must identify the weaknesses involved and describe the plans for corrective action.

B.2.2a Paperwork Reduction Act(PL96-511, December 11, 1980) [PRA80]: This Act imposes Federal information policy-making responsibilities on the Director of the Office of Management Budget (OMB) and requirements on Federal agencies to carry out these policies. Some of the more pertinent ones are:

- To develop and implement Federal information policies, principles, standards, and guidelines and to provide direction and oversee the review and approval of and acquisition and use of automatic data processing, telecommunications, and other technology for managing information resources.
- To evaluate agency information management practices to determine their adequacy and efficiency and to determine compliance with OMB information policies, principles, standards, and guidelines.
- To develop and implement policies, principles, standards, and guidelines on information disclosure and confidentiality, and on safeguarding the security of agency information.
- To monitor compliance with the Privacy Act of 1974.

B.2.2b Paperwork Reduction Reauthorization Act of 1986(PL99-591, October 30, 1986) [PRRA86]: This Act enhances and clarifies various sections of the original Paperwork Reduction Act of 1980. Some of the changes that are most pertinent to this report are:

- The term "information resources management" is added as a key definition and is defined as "the planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies, ..."
- OMB is explicitly given the responsibility to provide direction and oversee the review and approval of not only privacy but also security of records.
- OMB is to set a goal of reducing the burden of Federal information collections by at least 5% for each successive fiscal year from 1986 through 1989.
- Federal agencies are to implement the OMB directives generated by this Act.
- Federal agencies are to periodically evaluate, and, as needed, improve the accuracy, completeness, and reliability of data and records in Federal information systems.

B.2.3 Brooks Act(PL89-306, October 30, 1965) [BRA65]: The Federal ADP Standards program is authorized under this Act. It provides for the "economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies." Leadership roles for carrying out the goals of this Act are assigned to the Department of Commerce (DOC), the Office of Management and Budget (OMB), and the General Services Administration (GSA).

It authorizes the DOC to:

1. provide scientific and technological advisory services to other agencies for relating to automatic data processing and related systems;
2. make appropriate recommendations to the President concerning the establishment of uniform Federal automatic data processing standards; and
3. undertake research in computer science and technology as needed to fulfill the above responsibilities.

Under the Act, the OMB is responsible for exercising fiscal control and providing policy guidance to the Federal agencies on automatic data processing matters. The GSA is responsible for equipment procurement and maintenance. GSA reviews procurements and agency requests for services to assure that Federal Information Processing Standards (FIPS) are properly cited and used. The Act reserves to the agencies the authority to determine how computers will be used in accomplishing their missions.

B.2.4 Management of Federal Information Resources(OMB Circular A-130, (includes the revision to Transmittal Memo #1, OMB Circular A-71) December 12, 1985) [OMB130]: This calls for increased protection for Federal computers. OMB established, in 1978, a Federal computer security program to guard against illegal use of information stored in computers and to save taxpayer money. The program requires all executive branch departments and agencies to establish a management control and audit process for sensitive computer applications.

The program announced by OMB requires each executive department and agency to:

- Establish a management control process to assure that appropriate safeguards are built into all new computer applications.

- Assign responsibility for security of each new installation to a management official.

- Establish personnel security policies for both Federal and contractor personnel.

- Conduct periodic audits of all sensitive computer applications.

- Include security requirements in specifications for the acquisition or operation of computer facilities or related services.

- Conduct periodic risk analyses of each computer installation.

- Assure that appropriate contingency plans are developed to reduce the effect of computer breakdown, fires, or natural disasters.

B.2.5 The Privacy Act of 1974(PL93-579, December 31, 1974) [PYA74]: This Act defines the privacy of an individual as directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. In addition, the Act states that the increasing use of computers and sophisticated information technology has greatly magnified the harm to individual privacy. Verifying compliance to this Act is part of the audit function. The Act identifies which types of systems are included under the provisions of the Act. Basically, the Act covers those systems for which information is extracted by an individual identifier. The Act requires that systems covered under the Act be managed using good data management practices. From a compliance perspective, the Act identifies who may and may not have access to personal information. The Act identifies when the information of the individual must be obtained, and when information can be used without gaining permission of the individual involved. The Act also states the type of disclosure required by the agency responsible for the application system.

B.2.6 The Freedom of Information Act(PL90-23, June 5, 1967, as amended by PL93-502, November 21, 1974) [FIAA74]: This Act permits the public, except for specific categories of matters, to have access to information held by Federal agencies. The categories of matters not included are those that would impair rights of privacy or important government operations. The Act was primarily directed toward information maintained by the executive branch of the Federal government.

The agencies of the executive branch should inform the public where certain types of information may be obtained on request, and what internal agency appeals are available if a member of the public is refused requested information. Agency decisions to withhold identifiable records requested under the Act are subject to judicial review.

B.2.7a Internal Control Systems(OMB Circular A-123, October 28, 1981) [OMB123]: This Circular prescribes policies and standards to be followed by executive departments and agencies in establishing and maintaining internal controls in their program and administrative activities. It requires agency heads to:

- maintain effective systems of accounting and administrative control and
- have an internal control directive and a review plan in the form of a vulnerability assessment.

It requires agency Inspectors General, in conjunction with internal audit, to determine compliance with this Circular.

It states the internal control objectives are "to provide management with reasonable, but not absolute, assurance that financial and other resources are safeguarded from unauthorized use or disposition; transactions are executed in accordance with authorization; financial and statistical records and reports are reliable; applicable laws, regulations, and policies are adhered to; and resources are efficiently and effectively managed."

It specifies standards for system(s) of internal control, including: "documentation, recording of transactions, execution of transactions, separation of duties, adequate supervision, access to resources, competent personnel, and reasonable assurance."

B.2.7b Internal Control Systems(OMB Circular A-123 Revised, August 16, 1983) [OMBR123]: Circular A-123 was revised to incorporate the requirements of the Federal Managers' Financial Integrity Act [FMFIA82], OMB's Internal Control Guidelines [OMB82], and GAO's internal control standards [GAO83]. The most significant changes are:

- The responsibility section now specifies the internal control responsibilities of the designated senior internal control official and heads of organizational units to conform with OMB Internal Control Guidelines.
- Internal control objectives now conform with the Act.
- Internal control standards include those prescribed by GAO.
- Employees for whom performance agreements should include internal control responsibilities are defined.
- An agency's responsibility for taking timely corrective actions on weaknesses disclosed through its evaluation of internal controls is described.
- The Act's requirement for the agency head to submit an annual statement to the President and the Congress about the agency's system of internal control is included.

B.2.8 Financial Management Systems(OMB Circular A-127, December 19, 1984) [OMB127]: "This Circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems." The responsibilites specified include:

- "The head of each agency is responsible for ensuring that the planning, development, operation, review and reporting on the agency's financial management system are in accordance with this Circular.
- The manager of each financial system has responsibilities for performance of necessary system reviews and for issuance of reports thereon."
- The agency Inspector General should provide technical assistance and advice in the agency effort to review and improve the agency's financial management system.

- "Top agency management, as well as program and functional managers, shall participate in systems planning and evaluation to ensure that their needs are met."

Financial management systems objectives are spelled out. For systems operations, the best acceptably priced contemporary technology should be used to achieve systems that are useful, timely, provide reliable and complete information, use uniform definitions for comparability and consistency, and are efficient and economical. Reasonable controls for maintaining systems integrity should be used. The data in these systems should provide support for budget preparation, for managers to carry out their responsibilities, and to enable full financial disclosure as required.

B.2.9 Standards for Internal Controls in the Federal Government(Green Book), GAO, 1983 [GAO83]: This document contains the Comptroller General's internal control standards to be followed by executive agencies in establishing and maintaining systems of internal control as required by the Federal Manager's Financial Integrity Act of 1982 [FMFIA82]. These standards fall into three categories: General, Specific, and Audit Resolution.

The General standards consist of:

1. Reasonable Assurance that objectives of the systems will be accomplished;
2. Supportive Attitude maintained and demonstrated by managers and employees;
3. Competent Personnel who can accomplish their duties and understand need for good internal controls;
4. Control Objectives developed for each agency activity; and
5. Control Techniques are efficient and effective.

The specific standards consist of:

1. Documentation for internal control systems and all transactions and other significant events;
2. Recording of Transactions and Events promptly and properly classified;
3. Execution of Transactions and Events only by authorized persons;
4. Separation of Duties for authorizing, processing, recording, and reviewing transactions;
5. Supervision to ensure internal control objectives are achieved; and
6. Access to and Accountability for Resources by authorized individuals, with periodic review of accountability.

The Audit Resolution standard requires managers to promptly evaluate, determine the response to, and respond to audit findings.

APPENDIX C
KEY COMPUTER SECURITY AND AUDIT DEFINITIONS

The following key definitions in ADP internal control and computer security are provided to facilitate understanding of this guide.

1. Audit of computer security: A computer security audit is defined by NBS Special Publication 500-57[1] as:

> "An independent evaluation of the controls employed to ensure:
>
> 1. The appropriate protection of the organization's information assets (including hardware, software, firmware, and data) from all significant anticipated threats or hazards;
> 2. The accuracy and reliability of the data maintained on or generated by an automated data processing system; and
> 3. The operational reliability and performance assurance for accuracy and timeliness of all components of the automated data processing system."

2. Audit of internal controls: An independent evaluation of the internal controls related to the area being audited. The evaluation should develop an opinion relating to the adequacy of the internal controls to reduce risk to an acceptable level. Where internal controls are not acceptable, vulnerabilities should be identified. Auditing computer security is a subset of this activity.

3. Audit risk: Audit risks are the risks that are of concern to auditors.

4. Audit risk exposure: The possible forms of loss or harm that are of concern to auditors.

5. Audit risk exposure level: Proportional to the the probability of occurrence of the possible forms of loss that are of concern to auditors.

6. Computer generated risk: Computer generated risk is the potential loss or damage to an organization that results from the use or misuse of its computer. This may involve unauthorized disclosure, unauthorized modification, and/or loss of information resources as well as the authorized but incorrect use of a computer. This risk can be measured to some extent by performing a risk analysis. (Adapted from [NBS57], p.A-2)

---

1 [NBS57], p.A-3.

7. Computer security: The current, generally accepted definition of computer security is given in NBS Special Publication 500-57[2]:

> "Computer security is a state or condition that a computer system possesses.Computer security is never absolute. Rather, each system possesses security at some level. Computer security is provided by internal safeguards (built into the hardware and software) and external safeguards (physical and procedural) against possible threats. The level of computer security is dependent on the degree to which:
>
> 1. The computer system's components (including hardware, software, firmware, and data) are protected against all significant threats;
> 2. Data maintained on or generated by its data processing systems are accurate and reliable; and
> 3. Its data processing systems are operationally reliable and satisfy criteria that assure the accurate and timely performance of the system."

8. Control: Any protective action, device, procedure, technique, or other measure that reduces exposures. (FIPS102, p.61)

9. Exposure: A possible form of loss or harm, e.g., unauthorized disclosure, modification, destruction, or denial of service.

10. Internal control: Any method, procedure, or practice used to reduce the probability of loss or harm due to a flaw or weakness in the system. Note that various accounting publications define control for specific purposes, such as internal accounting controls are controls used to reduce financial risks.

11. Quality assurance: The planned, systematic process that ensures that automated system products and acquisition/development processes comply with established standards, practices, and procedures. Some of the quality assurance activities include lifecycle (a) validation, verification, and testing; (b) monitoring of development and testing activities, and change controls; (c) data integrity assurance; and (d) reviews and audits.

12. Risk: Risk is a potential damaging event which, if it occurs, can produce losses (see Section 1.2.1)

13. Risk analysis: Risk analysis is an analysis of an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate

2 Ibid.

of occurrence to establish a potential level of damage to assets or resources in terms of dollars or other assets.

14. System development life cycle (SDLC): A systematic method used for building automated information systems (AISs). This systematic process defines the activities and products/documents needed to create an AIS, and then divides the process into phases, assigning specific products/documents to each phase.

The SDLC phases adopted in this document are:

Initiation phase: This phase recognizes the users' need, validates that need, explores alternative functional concepts in order to recommend one for approval.

Definition phase: Defines the functional requirements and begins detailed planning for development of an operable AIS. The activities and goals for all phases, including resource estimates and milestones, are determined during this phase.

Systems design phase: This phase develops the specification of the problem solution. The detailed design specifications describe the physical solution in such a way that it can be implemented in code with little or no need for additional analysis.

Programming and training phase: This phase creates programs in accordance with the system design. During this phase, a training plan and documents, as well as user and maintenance manuals are prepared.

Evaluation and acceptance phase: During this phase, completed code will undergo testing to validate its performance. The security requirements need to be certified by an appropriate authority prior to accreditation and installation.

Installation and operation phase: This phase is designed to: 1)implement the approved operational plan, including extension to and installation at other sites; 2)continue approved operation; 3)budget adequately; and 4)control all changes and maintain/modify the AIS during its remaining life.

15. Vulnerability: A vulnerability is a design, implementation, or operations flaw that may be exploited by a threat, to cause the computer system or application to operate in a fashion different from its published specifications and to result in destruction or misuse of equipment or data. ([NBS57], p.A-2]

16. Vulnerability assessment: The process of (1)identifying flaws and the controls associated with those flaws in order to evaluate the adequacy of the control to reduce the riskes to an acceptable level; and (2)identifying those flaws for management action where risk levels are found to be too high.

APPENDIX D
ADDITIONAL RISKS IN A COMPUTERIZED ENVIRONMENT

D.1 IMPROPER USE OF TECHNOLOGY

Computer technology provides systems analysts and programmers with a variety of processing capabilities. This technology must be matched to the needs of the user to optimize the implementation of those needs. A mismatch of technology and needs can result in an unnecessary expenditure of organizational resources.

One of the more common misuses of technology is the introduction of new technology prior to the clear establishment of its need. For example, many organizations introduce data base technology without clearly establishing the need for that technology. Experience has shown that the early users of a new technology frequently consume large amounts of resources during the process of learning how to use that new technology.

The type of conditions that lead to the improper use of technology include:

1. Early and/or premature user of new hardware technology;

2. Early user of new software technology;

3. Minimal planning for the installation of new hardware and software technology; and

4. Systems analyst/programmer improperly skilled in the use of technology.

D.2 REPETITION OF ERRORS

In a manual processing environment, errors are made individually. Thus, a person might process one item correctly, make an error on the next, process the next twenty correctly, and then make another error. In automated systems, the rules are applied consistently. Thus, if the rules are correct, processing is always correct, but if the rules are erroneous, processing will always be erroneous.

Errors can result from application programs, hardware failures, and failures in vendor-supplied software. For example, a wrong percentage may have been entered for FICA deductions. Thus, every employee for that pay period will have the wrong amount deducted for FICA purposes.

The conditions that cause repetition of errors include:

1. Insufficient program testing;

2. Inadequate checks on entry of master information; and

3. Failure to monitor the results of processing.

D.3 CASCADING OF ERRORS

The cascading of errors is the domino effect of errors throughout an application system. An error in one part of the program or application triggers a second yet unrelated error in another part of the application system. This second error may trigger a third error, and so on.

The cascading of error risk is frequently associated with making changes to application systems. A change is made and tested in the program in which the change occurs. However, some condition has been altered as a result of the change, which causes an error to occur in another part of the application system.

Cascading of errors can occur between applications. This risk intensifies as applications become more integrated. For example, a system that is accepting orders may be tied through a series of applications to a system that replenishes inventory based upon orders. Thus, an insignificant error in the order entry program can "cascade" through a series of applications resulting in a very serious error in the inventory replenishment program.

The types of conditions that lead to cascading of errors include:

1. Inadequately tested applications;

2. Failure to communicate the type and date of changes being implemented; and

3. Limited testing of program changes.

D.4 ILLOGICAL PROCESSING

Illogical processing is the performance of an automated event which would be highly unlikely in a manual processing environment, for example, producing a payroll check for a clerical individual for over $1 million. This is possible in an automated system due to programming or hardware errors, but highly unlikely in a manual system.

Computerized applications do not have the same human oversight as is incorporated into manual systems. In addition, fewer people have a good understanding of the processing logic of computerized applications. Thus, in some instances illogical processing may not be readily recognizable.

The conditions that can result in illogical processing include:

1. Failure to check for unusually large amounts on output documents;

2. Fields that are either too small or too large, thereby impacting the completeness, accuracy, or efficiency of the data being processed; and

3. Failure to scan output documents.

D.5 INABILITY TO TRANSLATE USER NEEDS INTO TECHNICAL REQUIREMENTS

One of the major failures of data processing has been a communication failure between users and technical personnel. In many organizations users cannot adequately express their needs in terms that facilitate the preparation of computerized applications. Likewise, the technical computer people are often unable to appreciate the concerns and requirements of their users.

The risk associated with failure to satisfy user needs is complex. Exposures include: (1) failure to implement needs because users were unaware of technical capabilities; (2) improperly implemented needs because the technical personnel did not understand user requirements; (3) users accepting improperly implemented needs because they are unsure how to specify changes; and (4) the building of redundant manual systems to compensate for weaknesses in computerized applications.

The conditions that can lead to the inability to translate user needs into technical requirements include:

1. Users without technical EDP skills;

2. Technical people without sufficient understanding of user requirements;

3. User's inability to specify requirements in sufficient detail; and

4. Multi-user systems with no user "in charge" of the system.

D.6 INABILITY TO CONTROL TECHNOLOGY

The problems associated with the implementation of new technology have absorbed most of the efforts of data processing personnel. The SAC study [IIA-77-1,2,3] implied that there was too little time left to develop and install technological controls. The result is expenditure of resources to correct technological problems.

Controls are needed over the technological environment. The controls ensure that the proper version of the proper program is in production at the right time, that the proper files are mounted, that operators perform the proper instructions, that adequate procedures are developed to prevent, detect, and correct problems occuring in the operating environment, and that the proper data is maintained and retrievable when needed. The types of conditions that result in uncontrolled technology include:

1. Selection of vendor-offered system control capabilities by systems programmers without considering audit needs;

2. Too many control tradeoffs for operational efficiency;

3. Inadequate restart/recovery procedures;

4. Inadequate control over different versions of programs;

5. Inadequate control over schedulers, system operators, tape librarians, print capabilities, and data transmission capabilities; and

6. Inadequate review of outputs.

D.7 INCORRECT ENTRY OF DATA

In computerized applications, there is a mechanical step required to convert input data into machine-readable format. In the process of conducting this task, errors can occur. Data that was properly prepared and authorized may be entered into computerized applications incorrectly.

Much of the data entered into batch type systems is entered using a keyboard device. Some of thse devices are keypunch machines and key-to-disk machines. The data originator manually transcribes the input information onto some type of form, and the form is given to a key operator to enter on computer media. During this keying process, errors are made.

In the newer technology, data can be originated and entered at the same time. For example, order entry clerks receive orders by telephone and key them directly into computer memory. However, errors can still occur during this process.

Other methods of data entry include optical scanners, process control computers that monitor situations such as production machinery, automatic cash dispensers and point-of-sale equipment. However, these are all mechanical devices and thus subject to failure.

The types of conditions that can cause incorrect entry of data include:

1. Human errors in keying data;

2. Mechanical failure of hardware devices;

3. Misinterpretation of characters or meaning of manually recorded input;

4. Misunderstanding of data entry procedures; and

5. Inadequate data verification procedures.

D.8 CONCENTRATION OF DATA

Computerized applications concentrate data in an easy to access format. In manual systems, data is voluminous and stored in many places. It is difficult for an unauthorized individual to spend much time browsing undetected through file cabinets or other manual storage areas.

Using computerized media, unauthorized individuals can browse using computer programs. This may be difficult to detect without adequate safeguards. In addition, the data can be copied quickly without leaving any visible trail or destroying the original data. Thus, the owners of the data may not be aware that the data has been compromised.

Data base technology increases the risk of data manipulation and compromise. The more data stored in a single place, the greater the value of that data to an unauthorized individual. For example, the information about an individual in the payroll application is restricted to current pay information, but when that data is coupled with personnel history, not only is current pay information available, but also pay history, individual skills, years of employment, progression of employment, and perhaps performance evaluation.

The concentration of data increases the problems of greater reliance on a single piece of data and reliance on a single computer file. If the data entered is erroneous, the more applications that rely on that piece of data, the greater the impact of the error. In addition, the more

applications that use the concentrated data, the greater the impact when that data becomes unavailable due to problems with either the hardware or software used for processing that data.

The conditions that can create problems due to the concentration of data in computerized applications include:

1. Erroneous data and its impact on multiple users of that data;

2. Impact of hardware and software failures that ordinarily make the data available to multiple users;

3. Inadequate access controls enabling unauthorized access to data; and

4. Inefficient use of system for data storage and/or retrieval, which may impact response time or computer capacity.

D.9 INABILITY TO REACT QUICKLY

Much of the value of computerized applications is the ability to satisfy user needs on a timely basis. Some of these needs are predetermined and reports are prepared on a regular basis to meet these needs. Other needs occur periodically which require special actions to satisfy. If the computerized application is unable to satisfy these special needs on a timely basis, redundant systems may be built for that purpose.

One of the measures of success of a computerized application is the speed with which special requests can be satisfied. Some of the newer on-line data base applications with a query language can satisfy some requests within a very short time span. On the other hand, some of the older batch-oriented applications may take several days or weeks to satisfy a special request. In some instances, the structuring of the application system is an inhibiting factor in satisfying requests. For example, if an auditor wanted all of the supporting information for a supply requisition in a tape batched system, the cost and difficulty of satisfying that request may be prohibitive. The reason is that the requisition could be spread over many weeks of processing, due to back orders, returned shipments, and shipping errors. The evidence supporting the transaction may be spread over many tape files and the cost of processing those files may be exhorbitant.

The conditions that can cause computerized applications to be unable to react quickly include:

1. Computer time is unavailable to satisfy the request, or computer terminals/-microcomputers are not readily accessible to users;

2. The structure of the computer files is inconsistent with the information requested;

3. General-purpose extract programs are not available to satisfy the desired request; and

4. The cost of processing exceeds the value of the information requested.

D.10 INABILITY TO SUBSTANTIATE PROCESSING

Computerized applications should contain the capability to substantiate processing. This substantiation includes both the ability to reconstruct the processing of a single transaction and the ability to reconstruct control totals. Computerized applications should be able to produce all of the source transactions that support a control total, and substantiate that any source document is contained in a control total.

Application systems need to substantiate processing for the purposes of correcting errors and proving the correctness of processing. When errors occur, computer personnel need to pinpoint the cause of those errors so they can be corrected. Computerized application customers, other users, and control-oriented personnel, such as auditors, frequently want to verify the correctness of processing.

The conditions that may result in the inability to substantiate processing include:

1. Evidence is not retained long enough;

2. The evidence from intermediate processing is not retained;

3. Evidence is not independently reviewed for quality assurance and/or data integrity;

4. Outputs are not reviewed for quality by the users; and

5. The cost of substantiating processing exceeds the benefits derived from the process.

D.11 CONCENTRATION OF RESPONSIBILITIES

The computerization of an application tends to concentrate the responsibilities of many people into the automated application. Responsibilities that had been segregated for control purposes among many people may be concentrated into a single application system. In addition, a single application system may concentrate responsibilities from many departments within an organization.

The responsibilities in a computerized environment may be concentrated in both the application system and computer-oriented personnel. For example, the data base administrator may absorb data control responsibilities from many areas in the organization. A single computer system project leader may have the processing responsibility for many areas in the organization. New methods of separation of duties must be substituted for the previous segregation of duties among people.

The conditions that cause the concentration of responsibilities in a computerized environment include:

1. The establishment of a data processing programming and systems group to develop computerized applications for an organization;

2. Centralized processing of computerized applications;

3. Establishment of a data base administration function;

4. The lack of adequate standards and enforcement of those standards; and

5. The lack of adequate quality assurance and systems or applications testing.

APPENDIX E
VULNERABILITIES IN A COMPUTERIZED ENVIRONMENT

The following five pages are an exact duplicate of the application system vulnerabilities list found in FIPS PUB 65, GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS. It is included here for the convenience of the reader.

1. ERRONEOUS OR FALSIFIED DATA INPUT. Erroneous or falsified input data is the simplest and most common cause of undesirable performance by an applications system. Vulnerabilities occur wherever data is collected, manually processed, or prepared for entry to the computer.

- Unreasonable or inconsistent source data values may not be detected.
- Keying errors during transcription may not be detected.
- Incomplete or poorly formatted data records may be accepted and treated as if they were complete records.
- Records in one format may be interpreted according to a different format.
- An employee may fraudulently add, delete, or modify data (e.g., payment vouchers, claims) to obtain benefits (e.g., checks, negotiable coupons) for himself.
- Lack of document counts and other controls over source data or input transactions may allow some of the data or transactions to be lost without detection—or allow extra records to be added.
- Records about the data-entry personnel (e.g., a record of a personnel action) may be modified during data entry.
- Data which arrives at the last minute (or under some other special or emergency condition) may not be verified prior to processing.
- Records in which errors have been detected may be corrected without verification of the full record.

2. MISUSE BY AUTHORIZED END USERS. End users are the people who are served by the ADP system. The system is designed for their use, but they can also misuse it for undesirable purposes. It is often very difficult to determine whether their use of the system is in accordance with the legitimate performance of their job.

- An employee may convert Government information to an unauthorized use; for example, he may sell privileged data about an individual to a prospective employer, credit agency, insurance company, or competitor; or he may use Government statistics for stock market transactions before their public release.
- A user whose job requires access to individual records in a file may manage to compile a complete listing of the file and then make unauthorized use of it (e.g., sell a listing of employees' home addresses as a mailing list).
- Unauthorized altering of information may be accomplished for an unauthorized end user (e.g., altering of personnel records).
- An authorized user may use the system for personal benefit (e.g., theft of services).
- A supervisor may manage to approve and enter a fraudulent transaction.
- A disgruntled or terminated employee may destroy or modify records—possibly in such a way that backup records are also corrupted and useless.
- An authorized user may accept a bribe to modify or obtain information.

3. UNCONTROLLED SYSTEM ACCESS. Organizations expose themselves to unnecessary risk if they fail to establish controls over who can enter the ADP area, who can use the ADP system, and who can access the information contained in the system.

- Data or programs may be stolen from the computer room or other storage areas.
- ADP facilities may be destroyed or damaged by either intruders or employees.
- Individuals may not be adequately identified before they are allowed to enter ADP area.
- Remote terminals may not be adequately protected from use by unauthorized persons.
- An unauthorized user may gain access to the system via a dial-in line and an authorized user's password.
- Passwords may be inadvertently revealed to unauthorized individuals. A user may write his password in some convenient place, or the password may be obtained from card decks, discarded printouts, or by observing the user as he types it.
- A user may leave a logged-in terminal unattended, allowing an unauthorized person to use it.
- A terminated employee may retain access to ADP system because his name and pass-

word are not immediately deleted from authorization tables and control lists.
- An unauthorized individual may gain access to the system for his own purposes (e.g., theft of computer services or data or programs, modification of data, alteration of programs, sabotage, denial of services).
- Repeated attempts by the same user or terminal to gain unauthorized access to the system or to a file may go undetected.

4. INEFFECTIVE SECURITY PRACTICES FOR THE APPLICATION. Inadequate manual checks and controls to insure correct processing by the ADP system or negligence by those responsible for carrying out these checks result in many vulnerabilities.
- Poorly defined criteria for authorized access may result in employees not knowing what information they, or others, are permitted to access.
- The person responsible for security may fail to restrict user access to only those processes and data which are needed to accomplish assigned tasks.
- Large funds disbursements, unusual price changes, and unanticipated inventory usage may not be reviewed for correctness.
- Repeated payments to the same party may go unnoticed because there is no review.
- Sensitive data may be carelessly handled by the application staff, by the mail service, or by other personnel within the organization.
- Post-processing reports analyzing system operations may not be reviewed to detect security violations.
- Inadvertent modification or destruction of files may occur when trainees are allowed to work on live data.
- Appropriate action may not be pursued when a security variance is reported to the system security officer or to the perpetrating individual's supervisor; in fact, procedures covering such occurrences may not exist.

5. PROCEDURAL ERRORS WITHIN THE ADP FACILITY. Both errors and intentional acts committed by the ADP operations staff may result in improper operational procedures, lapsed controls, and losses in storage media and output.

Procedures and Controls:
- Files may be destroyed during data base reorganization or during release of disk space.
- Operators may ignore operational procedures; for example, by allowing programmers to operate computer equipment.
- Job control language parameters may be erroneous.
- An installation manager may circumvent operational controls to obtain information.
- Careless or incorrect restarting after shutdown may cause the state of a transaction update to be unknown.
- An operator may enter erroneous information at CPU console (e.g., control switch in wrong position, terminal user allowed full system access, operator cancels wrong job from queue).
- Hardware maintenance may be performed while production data is on-line and the equipment undergoing maintenance is not isolated.
- An operator may perform unauthorized acts for personal gain (e.g., make extra copies of competitive bidding reports, print copies of unemployment checks, delete a record from journal file).
- Operations staff may sabotage the computer (e.g., drop pieces of metal into a terminal).
- The wrong version of a program may be executed.
- A program may be executed using wrong data or may be executed twice using the same transactions.
- An operator may bypass required safety controls (e.g., write rings for tape reels).
- Supervision of operations personnel may not be adequate during non-working hour shifts.
- Due to incorrectly learned procedures, an operator may alter or erase the master files.
- A console operator may override a label check without recording the action in the security log.

Storage Media Handling:
- Critical tape files may be mounted without being write protected.

- Inadvertently or intentionally mislabeled storage media are erased. In a case where they contain backup files, the erasure may not be noticed until it is needed.
- Internal labels on storage media may not be checked for correctness.
- Files with missing or mislabeled expiration dates may be erased.
- Incorrect processing of data or erroneous updating of files may occur when card decks have been dropped, partial input decks are used, write rings mistakenly are placed in tapes, paper tape is incorrectly mounted, or wrong tape is mounted.
- Scratch tapes used for jobs processing sensitive data may not be adequately erased after use.
- Temporary files written during a job step for use in subsequent steps may be erroneously released or modified through inadequate protection of the files or because of an abnormal termination.
- Storage media containing sensitive information may not get adequate protection because operations staff is not advised of the nature of the information content.
- Tape management procedures may not adequately account for the current status of all tapes.
- Magnetic storage media that have contained very sensitive information may not be degaussed before being released.
- Output may be sent to the wrong individual or terminal.
- Improperly operating output or post-processing units (e.g., bursters, decollators or multipart forms) may result in loss of output.
- Surplus output material (e.g., duplicates of output data, used carbon paper) may not be disposed of properly.
- Tapes and programs that label output for distribution may be erroneous or not protected from tampering.

6. PROGRAM ERRORS. Applications programs should be developed in an environment that requires and supports complete, correct, and consistent program design, good programming practices, adequate testing, review, and documentation, and proper maintenance procedures. Although programs developed in such an environment will still contain undetected errors, programs not developed in this manner will probably be rife with errors. Additionally, programmers can deliberately modify programs to produce undesirable side effects or they can misuse the programs they are in charge of.

- Records may be deleted from sensitive files without a guarantee that the deleted records can be reconstructed.
- Programmers may insert special provisions in programs that manipulate data concerning themselves (e.g., payroll programmer may alter his own payroll records).
- Data may not be stored separately from code with the result that program modifications are more difficult and must be made more frequently.
- Program changes may not be tested adequately before being used in a production run.
- Changes to a program may result in new errors because of unanticipated interactions between program modules.
- Program acceptance tests may fail to detect errors that only occur for unusual combinations of input (e.g., a program that is supposed to reject all except a specified range of values actually accepts an additional value).
- Programs, the contents of which should be safeguarded, may not be identified and protected.
- Code, test data with its associated output, and documentation for certified programs may not be filed and retained for reference.
- Documentation for vital programs may not be safeguarded.
- Programmers may fail to keep a change log, to maintain back copies, or to formalize recordkeeping activities.
- An employee may steal programs he is maintaining and use them for personal gain (e.g., sale to a commercial organization, hold another organization for extortion).
- Poor program design may result in a critical data value being initialized twice. An error may occur when the program is modified to change the data value—but only changes it in one place.
- Production data may be disclosed or

destroyed when it is used during testing.
- Errors may result when the programmer misunderstands requests for changes to the program.
- Errors may be introduced by a programmer who makes changes directly to machine code.
- Programs may contain routines not compatible with their intended purpose, which can disable or bypass security protection mechanisms. For example, a programmer who anticipates being fired inserts code into a program which will cause vital system files to be deleted as soon as his name no longer appears in the payroll file.
- Inadequate documentation or labeling may result in wrong version of program being modified.

7. OPERATING SYSTEM FLAWS. Design and implementation errors, system generation and maintenance problems, and deliberate penetrations resulting in modifications to the operating system can produce undesirable effects in the application system. Flaws in the operating system are often difficult to prevent and detect.
- User jobs may be permitted to read or write outside assigned storage area.
- Inconsistencies may be introduced into data because of simultaneous processing of the same file by two jobs.
- An operating system design or implementation error may allow a user to disable audit controls or to access all system information.
- The operating system may not protect a copy of information as thoroughly as it protects the original.
- Unauthorized modification to the operating system may allow a data entry clerk to enter programs and thus subvert the system.
- An operating system crash may expose valuable information such as password lists or authorization tables.
- Maintenance personnel may bypass security controls while performing maintenance work. At such times the system is vulnerable to errors or intentional acts of the maintenance personnel, or anyone else who might also be on the system and discover the opening (e.g., microcoded sections of the operating system may be tampered with or sensitive information from on-line files may be disclosed).
- An operating system may fail to record that multiple copies of output have been made from spooled storage devices.
- An operating system may fail to maintain an unbroken audit trail.
- When restarting after a system crash, the operating system may fail to ascertain that all terminal locations which were previously occupied are still occupied by the same individuals.
- A user may be able to get into monitor or supervisory mode.
- The operating system may fail to erase all scratch space assigned to a job after the normal or abnormal termination of the job.
- Files may be allowed to be read or written without having been opened.

8. COMMUNICATIONS SYSTEM FAILURE. Information being routed from one location to another over communication lines is vulnerable to accidental failures and to intentional interception and modification by unauthorized parties.

Accidental Failures:
- Undetected communications errors may result in incorrect or modified data.
- Information may be accidentally misdirected to the wrong terminal.
- Communication nodes may leave unprotected fragments of messages in memory during unanticipated interruptions in processing.
- Communication protocol may fail to positively identify the transmitter or receiver of a message.

Intentional Acts:
- Communications lines may be monitored by unauthorized individuals.
- Data or programs may be stolen via telephone circuits from a remote job entry terminal.
- Programs in the network switching computers may be modified to compromise security.
- Data may be deliberately changed by individuals tapping the line (requires some

sophistication, but is applicable to financial data).

- An unauthorized user may "take over" a computer communication port as an authorized user disconnects from it. Many systems cannot detect the change. This is particularly true in much of the currently available communication equipment and in many communication protocols.
- If encryption is used, keys may be stolen.
- A terminal user may be "spoofed" into providing sensitive data.
- False messages may be inserted into the system.
- True messages may be deleted from the system.
- Messages may be recorded and replayed into the system ("Deposit $100" messages).

APPENDIX F
EVIDENCE PROVIDED BY COMPUTER TECHNOLOGY

F.1 TRADITIONAL FORMS OF AUDIT EVIDENCE

The evidence produced by an AIS may be different than that produced by manual systems. It is important for the auditor to understand these new forms of evidence because the methods used for auditing will change as the forms of evidence change. The following is a listing of the traditional forms of evidence that exist when manual processing is used. The description provides an example of how the computer can change the forms of that evidence:

1. People-initiated transactions - Transactions originated by people and entered into a system for processing. In computerized applications, transactions can be automatically generated. For example, the application can automatically issue a replacement order when inventory falls below a reorder point.

2. Hard-copy input - The manual recording of the information needed to originate a transaction. In computerized applications information can be entered through a terminal, which leaves no hard document. For example, a pay rate change can be entered on a computerized payroll master file through a computer terminal.

3. Manual authorization - People, usually supervisors, review transactions and then affix their signature, initials, or stamp to the document indicating authorization for processing. In computerized applications, authorization can be predetermined. For example, sales on credit can be automatically approved if a predetermined credit limit is not exceeded. Other methods of electronic authorization include entering a password, inserting a magnetically-encoded card, or turning a supervisory key in a terminal.

4. Movement of documents - People carry documents from one workstation to another, or move the documents by mail or equivalent service from one place of business to another. By these methods, a physical document is moved. In computerized applications, the data can be sent electronically. The data is transcribed, coded, often condensed, and then moved electronically over communication lines.

5. Hard-copy processing - Processing is manually performed using the transaction documents. For example, a form might show the steps performed by a procurement officer in selecting a vendor. Normally the documents contain work space to perform the necessary processing. In computerized applications, processing is

done electronically within computer storage by computer programs following predetermined rules.

6. Simplified processing - The processing performed must be simplified so that people can perform the steps repetitively without a high probability of error. In computerized applications, processing can be extremely complex due to the speed and accuracy of the computer. For example, production scheduling can be calculated hundreds of different ways in order to select the most effective schedule.

7. Manuals of master information - The permanent-type information needed for processing, such as pay rates and product pricing, is maintained in manuals. For example, if GS pay rates by step are in manuals that evidence can be read by people. In computerized applications, this information is stored on computer media.

8. Hard-copy output - The results of processing are listed on hard-copy documents, such as checks and reports. Frequently these documents contain the intermediate processing results. In computerized applications, processing may not result in the production of hard-copy documents. For example, funds can be transferred electronically, output reports displayed on video screens. In some systems, routine information is withheld so that the recipient receives only exception items which require action.

9. File of documents - Input, processing, and output documents are stored in file cabinets or similar containers. When the data is needed, it can be manually located and retrieved from the physical storage area. In a procurement system, purchase orders might be stored in a file cabinet. In computerized applications, most files exist on computer media, such as tapes and disks. To retrieve data from these media requires the use of extract programs.

10. Hard-copy audit trail - The information needed to reconstruct processing is contained in hard-copy documents. These documents contain source data, the authorization signature, methods of processing, and output results. This is normally sufficient information to reconstruct the transaction and to trace the transaction to control totals, or from control totals back to the source document. For example, a payroll paper audit trail would permit the reconstruction of each employee's salary. In computerized applications, the audit trail may be fragmented, such as often occurs in a data base environment. Also, much of the audit trail information may be stored on computer media. Computerized audit trails frequently require the user of the audit trail to understand the rules of processing

because it may not be obvious which processing path was taken, especially when computer processing is complex.

11. Procedure manual - All of the steps needed to process transactions through a system are contained in one or more procedure manuals. These are guides for people in moving and processing transactions. For example, procedures might be developed to define the steps to follow when a transaction is outside normal processing, such as a claim for a nonreimbursed healthcare expense.

12. Manual monitoring - People, normally supervisors, oversee and review processing to determine its reasonableness, accuracy, completeness, and authorization. For example, a supervisor would review department purchase orders for correctness and need prior to sending them to procurement. In computerized applications, much of this monitoring is performed automatically using predetermined program logic. It is difficult to have people monitor processing as computer systems become more integrated and complex and the processing cycle is shortened.

13. Proof of segregation of duties - Segregation of duties occurs by dividing tasks among people. In computerized applications, segregation of duties not only involves the division of tasks among people, but the division of tasks among automated processing steps. For example, one computer program may process one part of a transaction, while another computer program processes a different part.

14. Bulk processing techniques - The processing of large amounts of data may involve re-sequencing or matching diverse data elements. This is often difficult and costly in a manual system, so it is only done when necessary. In computerized applications, large amounts of data can be stored in a single data base. The speed and processing capability of the computer makes this data available in any format desired. In a computerized environment, more complex analyses and secondary uses of data can be made.

F.2 IMPACT OF COMPUTER TECHNOLOGY ON EVIDENCE

The introduction of the computer may change the traditional forms of evidence. If this evidence changes, so must the methods of auditing change. Tools and techniques that are effective in a manual environment may not be applicable to audits in the computerized environment.

The forms of evidence that the auditor examines in a manual environment include:

1. Origination documents such as purchase orders, employee timecards, and requisition forms;

2. Approval evidence such as signatures, time stamps, and date stamps;

3. Processing evidence, including calculation forms, master data manuals, and adding machine tapes; and

4. Output evidence, including checks, bank statements, invoices and reports.

Understanding how computer technology impacts audit evidence enables the auditor to recognize and appreciate the need to audit differently in a computerized environment. This section will review the traditional forms of evidence in a manual environment and then identify the types of automated technology that may impact the traditional forms of evidence. This will assist auditors in determining whether they need to modify their audit methods because of the introduction of the computer.

F.3 IMPACT OF CHANGING EVIDENCE ON AUDIT

Most organizations subject to an audit function have a computer. In these organizations, most applications are computerized. Thus, the question the auditor must ask is, "Does the computer impact my audit?" The audit is impacted if the form of audit evidence is changed. This changed form of evidence can create new audit concerns, and at the same time require the auditor to use new audit methods to obtain and/or examine the evidence.

F.3.1 The Audit Dilemma

One can look at two implementations of a computerized payroll application to assess the audit impact of the computer on each implementation. An auditor is assigned to conduct an audit of a payroll application. The application is computerized and the auditor needs to design an audit strategy. The audit dilemma is what, if anything, is different about the audit because the application is computerized.

Case A - Computerized Payroll Application

Organization A computerized their payroll application. In this application, each employee fills out a timecard and the employee's supervisor signs the timecard approving the hours. The data is entered into the application on a key-to-disk machine, and a copy of the entered information is returned to the supervisor for verification. At the beginning of each pay

period, a listing is prepared of all changes to the payroll rates and deductions. Also, a detailed report is printed listing each employee's pay information, pay history, pay deductions, and wage status at the end of that pay period. Each department gets a report showing all the information used for preparing payroll, together with the results of that processing. The checks are printed and then distributed by each employee's supervisor. The endorsed checks are independently reconciled by personnel outside the payroll department.

This application has not significantly changed the traditional forms of evidence. Thus, the same methods used to audit a manual payroll system would be effective in the audit of this computerized payroll application. However, the auditor may wish to use automated audit methods, such as audit software, to improve the efficiency and economy of the audit.

Case B - Computerized Payroll Application

Organization B computerized their payroll application using data collection terminals. Employees were issued magnetically encoded cards and when they enter and leave work they insert these cards into the data collection equipment. This records employee start and stop times. The personnel department uses a terminal to enter payroll changes into a payroll data base. The effective date of the change is entered with the data so that information can be entered whenever available. The results of payroll processing are transmitted electronically to banks and deposited to employee accounts in that bank. The pay information is printed into sealed envelopes and mailed to the employee's home.

In this application, the forms of evidence have changed significantly. These new forms of evidence should raise audit concerns and cause the auditor to use new audit methods. Both cases represented computerized applications. The cases are provided to illustrate that the computer itself should not be the key concern to the auditor but, rather, the effect of the application on the audit evidence.

F.3.2 Changing Forms of Evidence

The method for assessing the impact of the computer on the audit is to review whether computer technology has changed the traditional forms of evidence. In Case A, the computer was introduced but the evidence did not change. Therefore, the computer had little or no impact on the audit. In Case B, there was a significant change in the forms of evidence, and thus the methods of auditing need to be changed accordingly.

Prior to undertaking an audit of a computerized application, the auditor should identify the type of technology used. For example, the auditor would identify whether or not data is stored on computer storage media, whether communication facilities are used, etc. Then, by using the Audit Impact Matrix (Figure F.1)1, the auditor can identify the type of evidence that may be impacted by that technology. The auditor should then investigate whether or not the audit evidence has, in fact, been impacted. For example, on-line input/output devices can impact the means of authorization. Knowing this, the auditor determines if, in fact, the methods of authorization have changed. If so, the auditor needs to consider whether this creates new audit concerns and/or necessitates new audit methods.

F.4 OBTAINING NEW FORMS OF EVIDENCE

Computer technology produces new forms of evidence. Much of the evidence is encoded on computer media and thus requires special effort to transcribe it into human-readable format. Other evidence is in the form of systems documentation. Special ADP skills may be needed in order to properly assess the completeness and usefulness of this documentation.

Figure F.2, entitled "Comparison of Old and New Forms of Evidence," is provided as a guide to auditors in identifying, obtaining, and assessing these new forms of evidence. The figure is not meant to be all-inclusive but, rather, representative of the types of new forms of evidence and the audit methods needed to obtain and utilize that evidence.

F.5 ANTICIPATING EVIDENCE AND RELATED CONTROLS

During AIS development, both managers and auditors must anticipate the evidence needed from the system to effectively discharge their responsibilities and thereby insure consideration is given to the related controls.

1 Figures F.1 and F.2 have been taken from [AUER86+], Appendix B-1, with permission.

Figure F.1. Audit Impact Matrix

Audit Evidence	Computer Technology						
	Input/ Output Devices		Communi-cations	Storage Media	Programming	Data Base	Systems Documentation
	Offline	Online					
People-initiated transactions					✓		
Hard copy input	✓	✓					
Manual authorization		✓			✓	✓	
Document transmission			✓				
Hard copy processing (simplified procedures)		(✓)	(✓)		(✓) ✓	(✓)	
Manuals of master information				✓			
Hard copy output	✓	✓		✓			
Documents filing				✓			
Hard copy audit trail			✓	✓		✓	
Procedure manuals							✓
Manual monitoring					✓		
Segregation of duties		✓	✓		✓	✓	
Large volume processing (accessibility/usability)		✓	✓	✓	✓	✓	

Figure F.2. Comparsion of Old and New Forms of Evidence

Traditional Form of Evidence	New Form of Evidence	Methods for Obtaining New Evidence
People-initiated transactions	Computer-generated transactions	Auditor must examine systems documentation and/or programs to review where and how the computer generates transactions. Transactions can be tested two ways: First, test data can be created for the program to determine whether transactions are correct and generated at the appropriate times. Second, using audit software, the auditor can extract the detailed records entering the program and the computer-generated transactions exiting the program. The auditor must then manually confirm whether the transaction was properly generated.
Hard copy input	Terminal-initiated input	Audit software can be used to sample a number of the input transactions; their authenticity must then be verified with the individual(s) responsible for entering them.
Manual authorization	Automatic or electronic authorization	Audit software can be used to prepare letters asking the individual responsible for the authorization to confirm that it was, in fact, valid.
Manual document transmission	Telecommunications	The auditor can extract all of the documents transmitted from one work station and compare them to an extract of the transactions received at another location.
Hard copy processing	Computer programming	There are several methods of verifying computer processing. First, test data can be run through the program and compared against manually calculated results. Second, the auditor can write a simulation routine and compare actual processing against running the same data through the simulation routine. Third, the auditor can flowchart the program using an automatic flow-charting routine and then "paper debug" the processing to determine that it is correct.
Master information manual	Computer master file	Using audit software, the auditor can extract a sample of master information records (e.g., product pricing information) and compare it to the authorization documents to enter that information.
Document filing	Computer file	The auditor can use audit software to extract needed information from the computer file to print as hard copy.
Procedure manuals	Data dictionary	The auditor can request printouts from the data dictionary to examine the data attributes.
Manual monitoring	Computer edits and audits	Erroneous test data can be entered into the computer to determine that the edit and audit routines prevent or detect those errors.
Segregation of duties	Division of automated processing	The auditor can use a transaction conflict matrix to verify that there is adequate separation among automated processing steps.

APPENDIX G
KEY REFERENCES - ANNOTATED

1. AUTOMATIC DATA PROCESSING AND TELECOMMUNICATIONS IN THE FEDERAL GOVERNMENT, Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503, January 1985 [OMB85]: This document is an annotated bibliography. Much of what is included here is new since 1982 and is likely to be under constant revision. Laws, policies, and regulations concerning ADP and telecommunications change rapidly and present a bewildering complexity to the uninitiated. Both government and the private sector are publishing increasing numbers of guides for keeping abreast of new technologies, systems, and products as aids in planning for the future. A complete and current bibliography is impossible to maintain.

The descriptions of laws and other documents listed herein are for information purposes only and should not be interpreted as policy statements in themselves.

The bibliography is arranged by issuing agency and type of document. A subject guide is also provided at the end of the document. Citations are generally arranged in reverse chronological order, with the most current materials listed first. Exceptions to this rule are numbered series of documents, which are listed in numerical order regardless of issue date. Numbered series, such as Federal Information Processing Standards, are not indexed in the subject guide and hence must be scanned separately. For major reports, annotations are provided.

2. ADP AUDIT GUIDE, VOLUME 2, GUIDELINES FOR AUDITS OF COMPUTER-BASED SYSTEMS UNDER DEVELOPMENT, U.S. Air Force Audit Agency, November 1, 1980 [AFAA80]: This audit guide provides guidelines for auditing computer-based systems under development. The guidelines explain the auditor's role, then provide a methodology for surveying the environment in which the system is being developed. The audit guide emphasizes the importance of allocating audit effort toward the high-risk areas. The guide is divided into two major parts: (1) project planning and management; and (2) system development project execution. These two parts are subdivided into the key aspects of those two areas, and then there are twenty chapters, one provided for each criterion, providing guidelines for evaluating that aspect of project planning and management, and system development project execution.

3. INFORMATION SYSTEMS AUDIT PROCESS, S. Rao Vallabhaneni, CPA, CMA, CISA, EDP Auditors Foundation, Inc., P.O. Box 88180, Carol Stream, IL 60188, 1983 [VALLS83]: This book is designed to provide adequate coverage of subject material for candidates taking the Certified Information Systems Auditor (CISA) examination, a program of the EDP Auditors Foundation. The book focuses on the substantive issues covered by the CISA ex-

amination. For general information such as examination study techniques, test-taking skills, sample examination questions and answers, development of the job dimensions, and administrative matters, please refer to the CISA Study Guide of January 1981.

The purpose of this reference is to demonstrate the skills needed to audit systems under development. Auditors lacking skills in any of the eleven job-dimension categories identified should obtain additional training in those areas prior to conducting audits of systems under development.

4. COMPUTER SYSTEM SECURITY (CSS) SCOPING FOR OPERATIONAL TEST AND EVALUATION (OT&E), The BDM Corporation, 1801 Randolph Road, SE, Albuquerque, NM 87106, October 31, 1984 [BDM84]: This report describes the scope of operational test and evaluation for computer system security. In audits of sensitive systems where security is important as a requirement, this document can be used to scope the nature of security problems, and then what type of operational test and evaluation needs to be taken based on those potential security risks. The book identifies security requirements and then indicates the type of tests that can be undertaken in each of those areas.

5. OFFICE OF INSPECTOR GENERAL AUDIT PLAN FOR REVIEWING DEVELOPMENTAL SYSTEMS, U.S. Department of the Interior, Office of Inspector General, 134 Union Blvd., Suite 520, Lakewood, CO 80228, 1986 [DOI86]: This audit plan proposes a three-phase approach to auditing developmental systems in the department. The three phases are intended to provide maximum oversight during the developmental process with minimum auditor involvement. The primary objectives of such an oversight role are to assure:

- Proposed systems are needed.
- Systems are properly justified, feasible, and cost beneficial.
- Systems development is properly planned and controlled.
- Users are fully involved and trained.
- Systems are adequately tested and converted in a controlled manner.
- All internal controls are adequate and work, including audit trails.
- Audit resources are conserved.

6. AUDITOR'S MANUAL FOR SYSTEMS DEVELOPMENT LIFE CYCLE REVIEWS, Bureau of Government Financial Operations, Department of the Treasury, Office of Inspector General [DOTR-1]: The purpose of this manual is to create a structured approach to systems development life cycle (SDLC) audits. The authors researched existing publications on the subject and consulted organizations that conduct training in this area. From these sources, the authors were able to develop a methodology that detailed the audit objectives and techniques required to carry out an effective review of the development of a system throughout its life cycle. The auditor should look at this manual not as a cookbook for performing SDLC

audits but as a guide for effectively developing a structured audit approach geared to the specifics of the systems development project under review.

Before the auditor can use this manual as a guide to structure an audit program, the specific objectives, parameters, and constraints of the systems development project under review must be clearly identified. In other words, the auditor must understand the system before he can determine the structure of the audit program. As was detailed in the introduction, the primary function of an audit is to assure management that the system has adequate internal controls, meets identified objectives and user requirements, and is auditable.

7. REVIEW OF NEW OR MODIFIED DESIGN, Department of the Treasury, Office of the Inspector General, Bureau of the Public Debt [DOTR-2]: This audit guide is based on the six objectives of the additional GAO audit standard on audit involvement in systems development (Appendix I in GAO81-1). For each of the following seven phases, the audit guide provides a brief summary of what the auditor should do, followed by detailed audit checklists: (1) systems planning, (2) user specifications, (3) technical specifications, (4) program development and testing, (5) user procedures and training, (6) systems testing, and (7) conversion/implementation.

8. SYSTEM REVIEW AUDIT GUIDELINES, Richard P. Bush, George W. Steffen, Thomas M. O'Callaghan, Auditing Department, Federal Reserve Bank of Chicago, October 1981 [FRB81]: This audit guide keys the auditor involvement in systems development to specific control objectives. The guidelines do not attempt to tell an auditor what steps to follow when auditing a system development project. Rather, they point out the most important objectives of the process and leave it to the auditor to determine the degree of attention to these objectives. All objectives included in this set of guidelines are viewed to be critical to the system development process. A prudent auditor would therefore give appropriate consideration to all of these objectives when reviewing a system development project.

It is expected that an auditor will use these guidelines as a basis for developing detailed audit procedures for reviewing system development projects. The authors of this document believe that the decision as to the type and extent of audit procedures employed is best left to the audit function performing the review.

9. MULTI-AGENCY - ADP SYSTEM DEVELOPMENT LIFE CYCLE PROCESS, U.S. Department of Agriculture, Office of Inspector General, Washington, DC August 1983 [DOA83]: This document explains the system development life cycle process, from the perspective of what should be included in each life cycle phase. Knowing this information, the auditor is then informed as to what to look for during an audit of a system under development.

This audit guide is provided for use by OIG auditors involved in the review of automated system development activities. This guide was developed to provide a consistent approach within OIG for monitoring ADP systems development. This guide should be used for all audits which involve the monitoring of an ongoing system development effort or the review of an operational system from a development standpoint.

10. EVALUATING INTERNAL CONTROLS IN COMPUTER-BASED SYSTEMS, U.S. Government Accounting Office, June 1981 [GAO81-3]: This guide is intended to help auditors make a detailed review and evaluation of internal controls in computer-based systems. It includes the kinds of controls an auditor should expect to find in computer-based systems but does not try to establish standards for specific combinations of controls that should be used. Therefore, any one system would not include all the kinds of controls in the guide.

Detailed procedures are presented in sections as follows:

- Initial data collection
- Identification and evaluation of internal controls
- Detailed analysis and testing of controls and records
- Reporting and recommendations

It is not intended that all sections be applied to every audit. Questionnaires, checklists, internal control profiles, and internal control matrices are also included.

11. A STANDARD FOR AUDITING COMPUTER APPLICATIONS, William E. Perry, AUERBACH Publishers, 6560 N. Park Avenue, Pennsauken, NJ [AUER86+]: This audit guide is directed primarily at audits of operational systems. It presents an EDP audit in step-by-step format. However, the manual contains specialized sections, for example, a section on data base controls, that should prove beneficial in applications using these technologies. Also, the detailed operational programs should be beneficial in evaluating the adequacy of controls during development.

All large CPA firms have their own audit guidelines. For example, Arthur Andersen issued "A Guide for Studying and Evaluating Internal Accounting Controls;" and Touche Ross & Company has the "Touche Ross Audit Process." Generally, these are available from the CPA firms. Auditors should inquire of the firms auditing governmental agencies as to what audit guides they have available, and request them if the firms make them available to their clients or other interested parties.

12. STANDARDS FOR AUDIT OF GOVERNMENT ORGANIZATIONS, PROGRAMS, ACTIVITIES, AND FUNCTIONS, GAO, 1981 Revision [GAO81-1]: This document contains the standards to be followed by Federal auditors in performing their independent audit

function. Auditing scope encompasses three areas: financial and compliance; economy and efficiency; and program results. The four general standards relating to the scope of audit work are auditor qualifications, independence, due professional care, and scope impairments. This standards document also includes an appendix providing guidelines for the auditor's role during system development, design, and modification.

13. AUDITING COMPUTER SYSTEMS, FTP Technical Library, Port Jefferson Station, N.Y. 11776, 1981 plus updates [FTP81+]: This extensive manual is currently in four volumes and covers the computer audit field. Volume II addresses audit participation in the design of systems, system conversion, and system and program change.

14. INTERNAL CONTROLS, FTP Technical Library, Port Jefferson Station, N.Y. 11776, 1980 plus updates [FTP80+]: This manual explains how controls should be built into automated information systems. It includes an appendix which describes the functioning of over 500 different controls.

15. EDPACS (EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER), Automation Training Center, Inc., Reston, Virginia 22090 [EDPACS]: EDPACS is a monthly newsletter on EDP audit, control, and security topics. The newsletter normally contains at least one extensive article on a specific EDP audit or security topic. The remainder of the newsletter is usually devoted to a summarization of the recent literature on the topics of EDP audit, control, and security.

16. STANDARDS FOR INTERNAL CONTROLS IN THE FEDERAL GOVERNMENT, U.S. General Accounting Office (GAO), 1983 [GAO83]: This document defines standards for internal controls in the U.S. Federal Government. It is designed as a document to assist Federal managers in complying with the Federal Manager's Financial Integrity Act of 1982. The Act defines five general standards, six specific standards, and an audit resolution standard. The five general standards are reasonable assurance, supportive attitude, competent personnel, control objectives, and control techniques. The specific standards are documentation, recording of transactions and events, execution of transactions and events, separation of duties, supervision, and access to and accountability for resources. The audit resolution standard addresses prompt resolution of audit findings.

17. SYSTEM DEVELOPMENT MONITORING PROGRAM, U.S. Department of Labor, Office of Inspector General, Washington Regional Office, 1987 [DOL87]: This document was developed by the Office of Audits in the Office of Inspector General of the Department of Labor. The monitoring methodology uses three phases:

Phase I:	Pre-Survey
Phase II:	Survey
Phase III:	System Development Monitoring

The Pre-Survey allows the auditor to develop a picture of the general development environment while the Survey allows the auditor to identify worksteps for System Development Monitoring. The System Development Monitoring is divided into seven modules: Planning and Initiation, Acquisition and Procurement, Project Administration, System Design and Development, Programming, Testing and Conversion, and Implementation. The first two phases and the seven modules of the third phase each contain a series of worksteps for the auditor with a detailed data gathering instrument for each workstep. Appendices on reporting requirements, key terms, and key criteria are also included.

18. MODEL FRAMEWORK FOR MANAGEMENT CONTROL OVER AUTOMATED INFORMATION SYSTEMS, President's Council on Management Improvement and President's Council on Integrity and Efficiency, (Draft) August 1987 [PCMIIE]: This report synthesizes for managers the multitude of directives which contain overlapping and sometimes confusing guidance on how to protect automated information systems operations. It presents a model framework to help managers establish internal controls and document compliance for these systems. The framework has:

1. An analysis of Governing Directives that Federal Managers must follow. This yielded a set of 55 Control Requirements derived from Governing Directives.
2. A life cycle approach to assure that the Control Requirements have been met by the system under review at each phase of the life cycle.
3. A document flow analysis that parallels the phases of the life cycle and gives the auditor a means of checking that the Control Requirements have been met.

The life cycle phases and the documents for each phase are based on the work of the PCIE and can be found in greater detail in Chapter 2 of the present audit guide.

APPENDIX H
BIBLIOGRAPHY

AFAA80 — ADP Audit Guide, Volume 2, Guidelines for Audits of Computer-Based Systems Under Development, U.S. Air Force Audit Agency, November 1, 1980.

AICPA78 — Tentative Report of the Special Advisory Committee on Internal Accounting Control, American Institute of Certified Public Accountants, 1211 Avenue of the Americas, New York, NY 10036, September 15, 1978.

AUER86+ — A Standard for Auditing Computer Applications, William E. Perry, Auerbach Publishers, Inc., 6560 N. Park Ave., Pennsauken, New Jersey 08109, 1986 + updates.

BAPA50 — Budget and Accounting Procedures Act ot 1950, PL81-784, September 12, 1950.

BDM84 — Computer System Security (CSS) Scoping for Operational Test and Evaluation, The BDM Corporation, 1801 Randolph Road, SE, Albuqerque, NM 87106, October 31, 1984.

BOEMB81 — Boehm, Barry W., Software Engineering Economics, Prentice-Hall, Inc., Englewood Cliffs, NJ 07632, 1981.

BRA65 — Brooks Act, PL89-306, October 30, 1965.

C&L86 — System Develpment Audit Review Guide, by Coopers & Lybrand, 1251 Avenue of the Americas, New York, New York 10020, Publisher: Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, Florida 32701, September 1986.

DOD77 — Automated Data Systems Documentation Standards, DOD-STD-7935, September 13, 1977.

DOD78-1 — Life Cycle Management of AISs, DOD Directive 7920.1, October 17, 1978.

DOD78-2 — Major AIS Approval Process, DOD Instruction 7920.2, October 20, 1978.

DOI86 Office of Inspector General Audit Plan for Reviewing Developmental Systems, U.S. Department of Interior, Office of Inspector General 134 Union Blvd., Suite 520, Lakewood Co 80228, 1986.

DOL87 System Development Monitoring Program, U.S. Department of Labor, Office of Inspector General, Washington Regional Office, 1987.

DOT86 ADP Internal Control and Vulnerability Assessment Guidelines, Office of Information Systems and Telecommunications and Office of Financial Management, Department of Transportation, April 1986.

DOTR-1 Auditor's Manual for Systems Development Life Cycle Reviews, Bureau of Government Financial Operations, Department of the Treasury, Office of Inspector General.

DOTR-2 Review of New or Modified Design, Department of the Treasury, Office of Inspector General, Bureau of the Public Debt.

EAF83 Control Objectives-1983, EDP Auditors Foundation, Inc., P.O. Box 88180, Carol Stream, IL 60188, 1983.

FIAA74 Freedom of Information Act, PL90-23, June 5, 1967, as amended by PL93-502, November 21, 1974.

FIPS21-2 COBOL (ANSI X3.23-1985), FIPS PUB 21-2, National Bureau of Standards, March 18, 1986.

FIPS38 Guidelines for Documentation of Computer Programs and Automated Data Systems, FIPS PUB 38, National Bureau of Standards, February 15, 1976.

FIPS64 Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, FIPS PUB 64, National Bureau of Standards, August 1, 1979.

FIPS65 Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65, National Bureau of Standards, August 1, 1979.

FIPS68-2 BASIC (ANSI X3.113-1987), FIPS PUB 68-2, National Bureau of Standards, August 28, 1987.

FIPS69-1 FORTRAN (ANSI X3.9-1978), FIPS PUB 69-1, National Bureau of Standards, December 24, 1985.

FIPS73 Guidelines for Security of Computer Applications, FIPS PUB 73, National Bureau of Standards, June 30, 1980.

FIPS87 Guidelines for ADP Contingency Planning, FIPS PUB 87, National Bureau of Standards, March 27, 1981.

FIPS101 Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, FIPS PUB 101, National Bureau of Standards, June 6, 1983.

FIPS102 Guidelines for Computer Security Certification and Accreditation, FIPS PUB 102, National Bureau of Standards, September 27, 1983.

FIPS105 Guideline for Software Documentation Management, FIPS PUB 105, National Bureau of Standards, June 6, 1984.

FIPS106 Guideline on Software Maintenance, FIPS PUB 106, National Bureau of Standards, June 15, 1984.

FIPS109 PASCAL (ANSI/IEEE 770X3.97-1983), FIPS PUB 109, National Bureau of Standards, January 16, 1985.

FIPS110 Guideline for Choosing a Data Management Approach, FIPS PUB 110, National Bureau of Standards, December 11, 1984.

FIPS123 Specification for a Data Descriptive File for Information Interchange (DDL) (ANSI/ISO 8211-1985), FIPS PUB 123, Nstional Bureau of Standards, September 19, 1986.

FIPS126 Database Language NDL (ANSI X3.133-1986), FIPS PUB 126, National Bureau of Standards, March 10, 1987.

FIPS127 Database Language SQL (ANSI X3.135-1986), FIPS PUB 127, National Bureau of Standards, March 10, 1987.

FIPS128 Computer Graphics Metafile (CGM) ANSI X3.122-1986), FIPS PUB 128, National Bureau of Standards, March 16, 1987.

FIPS132 Guideline for Software Verification and Validation Plans (ANSI/IEEE 1012-1986), FIPS PUB 132, National Bureau of Standards, November 19, 1987.

FIRMR84 Management of ADP Resources, FIRMR 201-30.007, General Services Administration, December 21, 1984. [This is part of FIRMR Bulletin 15.]

FMFIA82 Federal Managers' Financial Integrity Act of 1982, PL97-255, September 8, 1982.

FRB81 System Review Audit Guidelines, Richard P. Bush, George W. Steffen, Thomas M. O'Callaghan, Auditing Department, Federal Reserve Bank of Chicago, October 1981.

FRMA50 Federal Records Management Act, PL81-754, 1950.

FRMA76 Federal Records Management Act, PL94-575, 1976.

FTP80+ Internal Controls, FTP Technical Library, Port Jefferson Station, New York 11776, 1980 + updates.

FTP81+ Auditing Computer Systems, FTP Technical Library, Port Jefferson Station, New York 11776, 1981 + updates.

GAO79-1 Data Base Management Systems--Without Careful Planning There Can Be Problems, U.S. General Accounting Office, June 29, 1979. FGMSD-79-35.

GAO79-2 Contracting for Computer Software Development--Serious Problems Require Management Attention to Avoid Wasting Additional Millions, U.S. General Accounting Office, November 9, 1979. FGMSD-80-4

GAO81-1 Standards for Audit of Governmental Organizations, Programs, Activities, and Functions, "Yellow Book", U.S. General Accounting Office, 1981 Revision.

GAO81-2 Federal Agencies' Maintenance of Computer Programs: Expensive and Undermanaged, U.S. General Accounting Office, February 26, 1981. AFMD-81-25.

GAO81-3 Evaluating Internal Controls in Computer-Based Systems "Black Book", U.S. General Accounting Office, June 1981. AFMD-81-76.

GAO81-4 Assessing Reliability of Computer Output, U.S. General Accounting Office, June 1981. AFMD-81-91.

GAO83 Standards for Internal Controls in the Federal Government, "Green Book", General Accounting Office, 1983.

GSACFR1 ADP Management Programs, 41 CFR 201-20, General Services Administration.

GSACFR2 Contracting for ADP Resources, 41 CFR 201-32, General Services Administration.

GSACFR3 Requirements Analysis, 41 CFR 210-20.003, General Services Administration.

GSA81-1 Software Improvement - A Needed Process in the Federal Government, General Services Administration, June 1981.

GSA81-2 Conversion Contracting Techniques Associated with Procurement of a Replacement ADP Hardware System, General Services Administration, Seprember 1981.

GSA82-1 A Software Tools Project: A Means of Capturing Technology and Improving Engineering, General Services Administration, February 1982.

GSA82-2 Conversion Work Packages, General Services Administration, July 1982.

GSA83-1 Conversion Plan Outline, General Services Administration, January 1983.

GSA83-2 Software Conversion Lessons Learned, Volume I, General Services Administration, January 1983.

GSA83-3 Guidelines for Planning and Implementing a Software Improvement Program (SIP), General Services Administration, May 1983.

GSA83-4 Establishing a Software Engineering Technology (SET), General Services Administration, June 1983.

GSA83-5 The Software Improvement Process--Its Phases and Tasks (Parts 1 & 2), General Services Administration, July 1983.

GSA84-1 Preparing Software Conversion Studies, General Services Administration, January 1984.

GSA84-2 Software Tool Evaluation and Selection Guidelines, General Services Administration, August 1984.

GSA85 Software Aids and Tools Survey, General Services Administration, November 1985.

GSA86-1 Conversion Cost Model (Version 4), General Services Administration, May 1986.

GSA86-2 Programmers Workbench Handbook, General Services Administration, June 1986.

GSA86-3 Information Systems Planning Handbook, General Services Administration, December 1986.

IEEE83-1 Standard Glossary of Software Engineering Terminology, ANSI/IEEE Std 729-1983.

IEEE83-2 Standard for Software Configuration Management Plans, ANSI/IEEE Std 828-1983.

IEEE83-3 Standard for Software Test Documentation, ANSI/IEEE Std 829-1983.

IEEE84-1 Standard for Software Quality Assurance Plans, ANSI/IEEE Std 730-1984.

IEEE84-2 Guide to Software Requirements Specifications, ANSI/IEEE Std 830-1984.

IEEE86-1 Standard for Software Unit Testing, ANSI/IEEE Std 1008-1986.

IEEE86-2 Standard for Software Verification and Validation Plans, ANSI/IEEE Std 1012-1986.

IGA78 Inspector General Act of 1978, PL95-452, October 12, 1978.

IIA77-1 Systems Auditability and Control, Data Processing Audit Practices Report, The Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, 1977.

IIA77-2 Systems Auditability and Control, Data Processing Control Practices Report, The Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, 1977.

IIA77-3 Systems Auditability and Control, Executive Report, The Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, 1977.

NBS57 Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, Edited by Zella G. Ruthberg, NBS Special Publication 500-57, National Bureau of Standards, April 1980.

NBS98 Planning for Software Validation, Verification, and Testing, Edited by Patricia B. Powell, NBS Special Publication 500-98, National Bureau of Standards, November 1982

NBS105 Guide to Software Conversion Management, Edited by M. Skall, NBS Special Publication 500-105, National Bureau of Standards, October 1983.

NBS133 Technology Assessment: Methods for Measuring the Level of Computer Security, William Neugent, John Gilligan, Lance Hoffman, Zella G. Ruthberg, NBS Special Publication 500-133, National Bureau of Standards, October 1985.

NBS136 An Overview of Computer Software Acceptance Testing, Delores R. Wallace, NBS SP 500-136, National Bureau of Standards, February 19, 1986.

NBSIR86 Work Priority Scheme for EDP Audit and Computer Security Review, Zella G. Ruthberg and Bonnie Fisher-Wright, National Bureau of Standards Internal Report, NBSIR 86-3386, March 1986.

OMB73 Audit of Federal Operations and Programs, OMB Circular A-73 (Revised), Office of Management and Budget, June 20, 1983.

OMB82 Internal Control Guideline, Office of Management and Budget, December 1982.

OMB85 Automatic Data Processing and Telecommunications in the Federal Government, Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503, January 1985.

OMB123 Internal Control Systems, OMB Circular A-123, Office of Management and Budget, October 28, 1981.

OMBR123 Internal Control Systems, OMB Circular A-123 Revised, Office of Management and Budget, August 16, 1983.

OMB127 Financial Management Systems, OMB Circular A-127, Office of Management and Budget, December 19, 1984.

OMB130 Management of Federal Information Resources, OMB Circular A-130, Office of Management and Budget, December 12, 1985.

PCIE86 Quality Standards for Federal Offices of Inspector General, by President's Council on Integrity and Efficiency (PCIE), 1986.

PCMIIE Model Framework for Management Control Over Automated Information Systems, President's Council on Management Improvement and President's Council on Integrity and Efficiency, (Draft), August 1987.

PRA80 Paperwork Reduction Act of 1980, 44 U.S.C. 3501, PL96-511, December 11, 1980

PRRA86 Paperwork Reduction Reauthorization Act of 1986, PL99-591, October 30, 1986.

PYA74 Privacy Act of 1974, 5 U.S.C. 552, PL93-579, December 31, 1974.

VALLS83 Vallabhaneni, S. Rao, Information Systems Audit Process, EDP Auditors Foundation, Inc., P.O. Box 88180, Carol Stream, IL 60188, 1983.

APPENDIX I
PCIE/NBS INVITATIONAL WORKSHOP

CO-CHAIRPERSONS: Bonnie T. Fisher & Zella G. Ruthberg

DISCUSSION GROUPS MEMBERSHIP

The following is a listing of the participants in the Invitational Workshop that resulted in the high level Risk Analysis presented in Chapter 3. This Risk Analysis is to be used for prioritizing the work of ADP auditors and security reviewers. The Workshop format used five discussion groups and the members are listed alphabetically for each group.

GROUP A

John Lainhart (Group Leader)	Department of Transportation Office of Inspector General Director, Office of ADP Audits and Technical Support
Robert L. Gignilliat (Recorder)	Department of Health and Human Services Senior Systems Security Officer
Nander Brown	Federal Home Loan Mortgage Corporation Assistant General Auditor
Peter S. Browne	Profile Analysis Corporation President
James E. Haines	Boeing Computer Services Co. Director, Quality Assurance
Kenneth Jannsen	Blue Cross/Blue Shield of Illinois Director, Internal Audits
Jarlath O'Neill-Dunne	Coopers and Lybrand, (New York, NY) Partner
Tyrone Taylor	National Aeronautics and Space Administration Space Station Management Analyst
John Van Borssum	Security Pacific National Bank Vice President, EDP Auditor
J. Armand Villemaire	Department of Defense Air Force Audit Agency, Staff Auditor
Patricia D. Williams	Department of Treasury Internal Revenue Service Head of Security

GROUP B

Barry R. Snyder (Group Leader)	General Accounting Office, IMTEC Group Director, Technical Services
Mark J. Gillen (Recorder)	Department of Treasury Internal Revenue Service Internal Audit Manager
Robert P. Abbott	EDP Audit Controls, Inc. President
Lorretta Ansbro	Federal Reserve Bank of New York Audit Official
Stephen F. Barnett	Department of Defense Computer Security Center Chief, Office of Application System Evaluation
Larry Bergman	Boeing Computer Services Co. EDP Audit Manager
Robert Berndt	Bank of America (San Francisco) Vice President, EDP Audit Manager
Keagle Davis	Touche Ross & Co. (Jacksonville) Partner
Michael Goldfine	General Motors Corporation Assistant Director, Audit Staff
Ralph E. Gooch	Department of Treasury Financial Management Services Chief of Security Branch
Michael G. Houston	Department of Defense Office of Inspector General Program Director, Audit Policy and Oversight
Jack Wheeler	General Accounting Office, IMTEC Special Assistant, Technical Services

GROUP C

Wallace O. Keene (Group Leader)	Department of Health & Human Services Acting Deputy Assistant Secretary for Management Analysis and Systems
Allen Winokur (Recorder)	Navy Audit Service EDP Auditor
David L. Decker	Department of Housing and Urban Development Office of Inspector General Director, EDP Audit
Frederick Gallegos	General Accounting Office (Los Angeles) Manager, Management Services Group
Carole A. Langelier	DeLoitte, Haskins and Sells (Washington, D.C.) Partner
Joseph T. McDermott	Department of Defense Office of Inspector General/AUDIT Program Manager
Gerald Meyers	EDP Audit Consultants Managing Partner
Carl A. Pabst	Touche Ross & Company (Los Angeles) Partner, Director of EDP Audit
Frederick G. Tompkins	ORI, Incorporated Senior Principal Scientist
Hart J. Will, Ph.D.	University of Victoria, B.C. Professor of Public Administration

GROUP D

Larry Martin (Group Leader)	Department of Energy Manager, Computer Security Program
Gail L. Shelton (Recorder)	Department of Health & Human Services Office of Inspector General Program Analyst
James Cox	Department of Health & Human Services Office of Inspector General EDP Auditor
Tim Grance, 2nd Lt.	U.S. Air Force Computer Security Program Office Computer Security Staff Officer
Michael J. Henitz	Peat Marwick Mitchell & Co. Computer Audit Office Partner
William M. Hufford	Sun Banks, Inc. Vice President, EDP Audit Manager; EDP Auditors Association Regional President
Stanley Jarocki	Bankers Trust of New York Vice President, Group Manager
William C. Mair	Touche Ross & Co. (Detroit) Partner
Thomas Nugent	Department of Navy, NARDAC Computer Specialist
Kenneth A. Pollock	EDP Auditors Foundation Director of Research
F. A. Schlegel	Management and Computer Services, Inc. President

GROUP D (continued)

D. L. Von Kleeck	Management and Computer Services, Inc. General Manager
H. C. Warner	Florida Power and Light Director, Internal Audits

GROUP E

Douglas B. Hunt (Group Leader)	National Aeronautics and Space Administration Office of Inspector General Director, Technical Services
William C. Lee (Recorder)	Department of Commerce Office of Inspector General Office of Automated Information Systems Computer Specialist
Philip Carollo	Sears, Roebuck and Company Director, EDP Audits
Don Colner	Basic Data Systems, Inc. President
Robert V. Jacobson	International Security Technology, Inc. President
Thomas Lux	Touche Ross & Company (Chicago) Audit Supervisor
Jim Manara	Security Pacific National Bank Quality Assurance Division Vice President
Brian McAndrew	U.S. Navy Navy Audit Service Assistant Director, Audit Policy
Brian Morse	Coopers & Lybrand (Washington, D.C.) Partner
Benson J. Simon	Environmental Protection Agency Program Analyst
Jane Tebbutt	Department of Health and Human Services Office of Inspector General Director, Interagency Projects Division

APPENDIX J
TWO RISK SCORING METHODS

J.1 A SIMPLE SCORING APPROACH

J.1.1 The Scoring Method

This method risk scores each system by using Figure J.1 to calculate the scores as described below.

Step 1 - Assign Importance Weights. A weight, reflecting the importance of the dimension to the system under review, is assigned to each of the five dimensions shown in Figure J.1. This weight will in turn reflect the importance of the dimension's characteristics to the system under review. One of the two suggested weighting schemes[1] shown in Figure J.1 can be used, although specific situations may require modification of these. The weights in set 1 add up to an arbitrary number while those in set 2 add up to 100. Set 2 allows for easy conversion of the weights to percentages.

Step 2 - Assign Risk Level. For each dimension assign a risk level from 1 - 5 which reflects the degree of risk for that dimension. Suggested risk level values are:

5 = High Risk
3 = Medium Risk
1 = Low Risk

For example, a system with demonstrated reliability would pose a low risk and warrant a low risk level value (=1).

Step 3 - Calculate Dimension Risk Score. The dimension risk score is its weight times its risk level.

Step 4 - Calculate System Risk Score. For a Level I type system risk score, use the risk score for the Criticality/Mission Impact dimension. The Level II system risk score is the sum of each of the five dimension's risk scores.

Step 5 - Rank System Scores. Perform Steps 2, 3, and 4 for each system under consideration and rank systems numerically from high to low. The highest scoring systems pose the highest risk and therefore deserve more audit/review attention.

---

1 The suggested weights were derived from data collected from representatives attending the PCIE Workshop.

Figure J.1. SYSTEM RISK SCORING - SIMPLIFIED METHOD

SYSTEM _____

Dimensions	Weight 1.	Weight 2.	Risk Level	Weighted Score	Comments
1. Criticality / Mission Impact	(20)	(50)			
2. Size / Scale / Complexity	(15)	(15)			
3. Environment / Stability	(10)	(10)			
4. Reliability / Integrity	(10)	(10)			
5. Technology Integration	(10)	(15)			
			System Score		

Table J.1. SYSTEM RISK SCORING - SIMPLIFIED METHOD EXAMPLE

SYSTEM Research Grants System

Dimensions	Weight 1.	Weight 2.	Risk Level	Weighted Score	Comments
1. Criticality / Mission Impact	20 (20)	(50)	8	160	Grants are major function; but manual operation is possible.
2. Size / Scale / Complexity	15 (15)	(15)	4	60	Size is small compared to all others.
3. Environment / Stability	10 (10)	(10)	3	30	It is a stand-alone system with known responsibilities and requirements.
4. Reliability / Integrity	10 (10)	(10)	8	80	There have been numerous instances of fraud in the present system.
5. Technology Integration	15 (10)	(15)	10	150	Will use the first data base package and a new communication method.
			System Score	480	

J.1.2 Example of a Scored System

Table J.1 is an example of a calculated risk score for one system. The suggested weights of set 1 in Figure J.1 were used except for Technology Integration. This was given a higher weight of 15 because, in the organization, almost all new systems have failed whenever any new technology is introduced. The five dimensions were then given a risk level value based on audit knowledge and surveys. A total score of 480 was then calculated for ranking purposes.

J.2 A DETAILED SCORING APPROACH

J.2.1 Risk Scoring a Dimension

Although the "strawman" paper describes five approaches to analyzing risk (See Appendix B in [NBSIR86]), a method of ranking and rating is suggested here as an approach commensurate with the softness of the data available. Each dimension of the scheme is rated and ranked separately, with scores then combined. Since Criticality/ Mission Impact is the Level I dimension of the proposed scheme, one would analyze this dimension first. The procedure is as follows:

First, the n characteristics within a dimension are ranked according to their respective importance to that dimension. The importance rank number of characteristic i is I(i) and ranges from 1 to n with n correlated with the most important characteristic. For operational systems one can use discriminant analysis applied to equal sets of known system failures and successes to obtain this ranking. For developmental systems a consensus view of audit management can be used, ideally obtaining Sponsor/User input.

Second, the importance ranking number, I(i), is converted to an importance weighting factor, W(i), that is normalized to 20. (The reason for selecting 20 will be explained in Section J.2.4.) This means that the sum of the weighting factors for the characteristics within a dimension is set to 20 (or normalized to 20). Since each of the five dimensions has a different number of characteristics and we wish to treat the dimensions as equals, normalization will guarantee that the risk score range for each dimension will be the same.

The normalization factor, F, is the number which converts the importance ranking number I(i) to the importance weighting factor W(i). The relationships are:

$$(1) \quad W(i) = F \times I(i)$$

$$(2) \quad \sum_{i=1 \text{ to } n} W(i) = \sum_{i=1 \text{ to } n} F \times I(i) = 20$$

Solving equation (2) for F, we find

$$(3) \quad F = \frac{20}{\sum_{i=1 \text{ to } n} I(i)}$$

and substituting for F in equation (1) yields the importance weighting factor W(i) for characteristic i, i.e.,

$$(4) \quad W(i) = 20 \times \frac{I(i)}{\sum_{i=1 \text{ to } n} I(i)}$$

Third, each characteristic is rated with respect to the risk of occurrence. One of the following risk ratings, R(i), is assigned to characteristic i.

R (i) = 3 (for High Risk)

R (i) = 2 (for Medium Risk)

R (i) = 1 (for Low Risk)

These ratings can be assigned by the auditor, again with user assistance if appropriate.

Finally, a Risk Score for that dimension is obtained by multiplying the importance weighting by the risk rating of the characteristic and summing over the characteristics for that dimension. The equation for this is the following:

$$DRS(j) = \sum_{i=1 \text{ to } n} W(i) \times R(i)$$

where i = characteristics 1 to n

W (i) = importance weighting for characterististic i

R (i) = risk rating for characteristic i

DRS (j) = dimension j's risk score, j = 1 to 5

The Risk Score for each of the five dimensions will range from 20 to 60 using these importance weighting and risk rating number assignments.

J.2.2 Level I System Risk Score

After completing a Level I review for an organization's universe of AISs, using the analysis scheme in Section J.2.1, one can use the Criticality/Mission Impact dimension risk score as a first order approximation to a system risk score. Since these risk scores have all been normalized to the same number (20), it is possible to compare these risk scores across AISs and eliminate from further consideration AIS's having a low risk with respect to Criticality/Mission Impact.

J.2.3 Level II Review Considerations

If it is decided that the more detailed Level II review is appropriate and/or affordable, one must decide upon a sequence for reviewing the remaining dimensions of the high risk critical AISs. While there is no "correct" way to do this, it might be appropriate to consider the following.

Since the Environment/Stability dimension includes the organization's general controls, including the strength and involvement of quality assurance, project management, and security functions throughout the SDLC (of both systems and major enhancements to existing systems), it may be most useful to review this dimension first in a Level II review. These general controls would heavily impact the need for audit coverage as well as the scope and expertise necessary in that coverage. The EDP auditors could confidently reduce their scope and related testing of applications if they could rely on the organization's general controls and the safeguards these various review functions provide in the SDLC process. Any ranking or prioritizing of the elements in the work priority scheme, beyond the overriding factors described above (i.e., external influence and mission criticality), could not be reasonably accomplished without a survey of the organization's general and applications controls and/or without an institutional knowledge of the organization, its SDLC process, and any facts and circumstances affecting system development activities. The characteristics in all four Level II dimensions should be weighted and rated in the light of such background information, and the dimension risk score, DRS, obtained for each of the four Level II dimensions.

J.2.4 Level II System Risk Score

As a second order approximation one can treat the dimensions as equal contributors to the risk score for the AIS as a whole. Under this assumption the system risk score, SRS, is then a simple sum of the five dimension risk scores, DRS.

$$(5) \quad SRS = \sum_{j=1 \text{ to } 5} DRS(j)$$

where SRS = system risk score

j = dimensions 1 to 5

DRS (j) = dimension j's risk score

Since DRS(j) can range from 20 to 60, SRS will range from 100 to 300. The choice of 20 for the sum of the weights of the characteristics within a dimension is arbitrary and was made in order to place SRS in a reasonable range for comparing one system's risk score to another's.

J.2.5 An Example

It may be a useful exercise to go through an example of the arithmetic involved. Assume we wish to calculate dimension risk scores and system risk scores for two AISs. To simplify matters we shall assume small numbers of characteristics for each dimension. Dimension 1 has four characteristics, dimension 2 has three characteristics, dimension 3 has five characteristics, dimension 4 has three characteristics and dimension five has 2 characteristics. The importance rankings I(i) and the risk ratings R(i) are obtained from audit management and the auditor respectively. The rest of the numbers in Tables J.2 and J.3 are calculated using equations (1) - (5). (A practice template of the table has been included in Figure J.2 to assist the reader in learning the methodology.)

Using dimension 1 as a first order system risk score, we find AIS 1, with DRS = 42, is more at risk than AIS 2, with DRS = 38. We obtain the second order risk score by adding the five dimension risk scores for each AIS. Using these numbers, AIS 1, with SRS = 191.4, is again more at risk than AIS 2, with its SRS = 180.0. Only experience with the method will enable the reviewer to obtain more refined interpretations of the calculations.

Figure J.2. PRACTICE TEMPLATE FOR RISK SCORING OF AN AIS

AIS _____

DIMENSION	I(i)	F	W(i)	R(i)	WxR	DRS(j)
DIM 1 C(1) C(2) C(3) C(4)						
DIM 2 C(1) C(2) C(3)						
DIM 3 C(1) C(2) C(3) C(4) C(5)						
DIM 4 C(1) C(2) C(3)						
DIM 5 C(1) C(2)						
					SRS	

Table J.2. DIMENSION RISK SCORES AND SYSTEM RISK SCORES FOR AIS 1

AIS 1

DIMENSION	I(i)	F	W(i)	R(i)	W x R	DRS(j)
DIM 1						
C(1)	2	2	4	1	4	
C(2)	1	2	2	2	4	
C(3)	4	2	8	2	16	
C(4)	3	2	6	3	18	
	10	-	20	-	42	42.0
DIM 2						
C(1)	3	10/3	10	1	10	
C(2)	2	10/3	20/3	2	40/3	
C(3)	1	10/3	10/3	3	10	
	6	-	20	-	33.3	33.3
DIM 3						
C(1)	4	4/3	16/3	3	16	
C(2)	2	4/3	8/3	2	16/3	
C(3)	5	4/3	20/3	1	20/3	
C(4)	1	4/3	4/3	2	8/3	
C(5)	3	4/3	4	3	12	
	15	-	20	-	42.7	42.7
DIM 4						
C(1)	1	10/3	10/3	3	10	
C(2)	3	10/3	10	3	30	
C(3)	2	10/3	20/3	1	20/3	
	6	-	20	-	46.7	46.7
DIM 5						
C(1)	1	20/3	20/3	2	40/3	
C(2)	2	20/3	40/3	1	40/3	
	3	-	20	-	26.7	26.7
					SRS	191.4

1st Order SRS (Range = 20 to 60) = DRS(1) = 42.0

2nd Order SRS (Range = 100 to 300) = SRS = 191.4

Table J.3. DIMENSION RISK SCORES AND SYSTEM RISK SCORES FOR AIS 2

AIS 2

DIMENSION	I(i)	F	W(i)	R(i)	W x R	DRS(j)
DIM 1						
C(1)	4	2	8	3	24	
C(2)	2	2	4	1	4	
C(3)	1	2	2	2	4	
C(4)	3	2	6	1	6	
	10	-	20	-	38	38.0
DIM 2						
C(1)	2	10/3	20/3	3	20	
C(2)	1	10/3	10/3	1	10/3	
C(3)	3	10/3	10	2	20	
	6	-	20	-	43.3	43.3
DIM 3						
C(1)	5	4/3	20/3	3	20	
C(2)	3	4/3	4	1	4	
C(3)	1	4/3	4/3	2	8/3	
C(4)	2	4/3	8/3	1	8/3	
C(5)	4	4/3	16/3	3	16	
	15	-	20	-	45.4	45.4
DIM 4						
C(1)	2	4	20/3	2	40/3	
C(2)	2	4	10	1	10	
C(3)	1	4	10/3	3	10	
	5	-	20	-	33.3	33.3
DIM 5						
C(1)	2	20/3	40/3	1	40/3	
C(2)	1	20/3	20/3	1	20/3	
	3	-	20	-	20	20.0
					SRS	180.0

1st Order SRS (Range = 20 to 60) = DRS(1) = 38.0
2nd Order SRS (Range = 100 to 300) = SRS = 180.0

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NBS/SP-500/153	2. Performing Organ. Report No.	3. Publication Date April 1988

4. TITLE AND SUBTITLE

Guide to Auditing for Controls and Security: A System Development Life Cycle Approach

5. AUTHOR(S) Zella G. Ruthberg, Bonnie Fisher-Wright, William E. Perry, John Lainhart, James G. Cox, Mark Gillen, Douglas B. Hunt

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

NBS and President's Council on Integrity and Efficiency
c/o Richard Kusserow, Inspector General, HHS
330 C. St. S. W.
Washington, DC 20201

10. SUPPLEMENTARY NOTES

This document is the result of a joint effort of ICST/NBS and a Work Group of the Computer Security Project of the President's Council on Integrity and Efficiency.

Library of Congress Catalog Card Number: 88-600518

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

This guide addresses auditing the system development life cycle (SDLC) process for an automated information system (AIS), to ensure that controls and security are designed and built into the system. It is directed toward mid-level ADP auditors having a minimum of two years experience in ADP auditing, but can also be used by security reviewers, quality assurance personnel, and as a training tool for less experienced ADP auditors. ADP managers and system developers will also find it useful guidance on security and control issues. It is designed to provide audit/review programs for each major phase of the SDLC process. It presents: (1) the model arrived at for describing the phases and functional roles in the entire AIS life cycle, (2) the accompanying flow of documents as the system progresses through the life cycle phases of Initiation, Definition, Design, Programming and Training, Evaluation and Acceptance, and Installation and Operation, (3) a security audit/review work priority scheme, and (4) audit/review programs for Initiation through Evaluation and Acceptance. The Installation and Operation phase is not treated because of already existing literature in this area. The guide represents the results of the past four years of activities by the Electronic Data Processing (EDP) Systems Review and Security Work Group of the Computer Security Project within the President's Council on Integrity and Efficiency (PCIE). It contains an annotated bibliography of important documents, a general bibliography, and a description of pertinent laws and regulations.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

Audit/review work priority scheme; automated information system; computer security review/audit; controls audit/review; controls/security regulations; life cycle documentation flow chart; phase audit tests; President's Council on Integrity and Efficiency; review/audit program; security/controls laws; system development life cycle model

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

266

15. Price

USCOMM-DC 6043-P80

☆ U.S. GOVERNMENT PRINTING OFFICE: 1988— 201-597/82557

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NBS Technical Publications

Periodical

Journal of Research—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).
NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.
Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*
Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Bureau of Standards
Gaithersburg, MD 20899

Stimulating America's Progress
1913-1988